

Mapping SVA to PSL

John Havlicek¹ Dana Fisman^{2,3} Cindy Eisner² Erich Marschner⁴

¹ Motorola, Inc.

² IBM Haifa Research Lab

³ Weizmann Institute of Science

⁴ Cadence, Inc.

Draft, 28 October 2003; PLEASE DO NOT DISTRIBUTE

Assumptions:

- The SVA semantics is understood to be from SVA 3.1, revised to include neutral semantics and to fix errata. The SVA neutral semantics is understood to be generalized to empty words, with the only change being that

$$\begin{aligned} w, b \models_{\text{sva}} \text{initial assert property } Q \\ \text{iff if } |w| > 0 \text{ and } \bar{w}^0 \models b, \text{ then } w \models_{\text{sva}} Q \end{aligned}$$

[Comments? Is this what people expect?]

- PSL semantics is understood to be from proposed PSL 1.1.

Restricted SVA Abstract Syntax

Note that local variables and `first_match` are not in the domain of the mapping. Throughout, “unlocked SVA sequence” means “unlocked SVA sequence without local variables or `first_match`”. Similarly, “clocked SVA sequence” means “clocked SVA sequence without local variables or `first_match`”.

In the following abstract grammars, b denotes a boolean expression, v denotes a local variable name, and e denotes an expression.

The abstract grammar for unlocked sequences is

```
R ::= b // “boolean expression” form
    | ( R ) // “parenthesis” form
    | ( R ##1 R ) // “concatenation” form
    | ( R ##0 R ) // “fusion” form
    | ( R or R ) // “or” form
    | ( R intersect R ) // “intersect” form
    | R[*0] // “null repetition” form
    | R[*1:$] // “unbounded repetition” form
```

The abstract grammar for clocked sequences is

```
S ::= @(b) R // “clock” form
    | ( S ## S ) // “concatenation” form
```

The abstract grammar for unlocked properties is

$$\begin{aligned}
 P ::= & \text{[disable iff } (b) \text{] [not] } R && // \text{ "sequence" form} \\
 & | \text{[disable iff } (b) \text{] [not] } (R \text{ } \dashv\rightarrow \text{ [not] } R) && // \text{ "implication" form}
 \end{aligned}$$

The abstract grammar for clocked properties is

$$\begin{aligned}
 Q ::= & @ (b) P && // \text{ "clock" form} \\
 & | \text{[disable iff } (b) \text{] [not] } S && // \text{ "sequence" form} \\
 & | \text{[disable iff } (b) \text{] [not] } (S \text{ } \dashv\rightarrow \text{ [not] } S) && // \text{ "implication" form}
 \end{aligned}$$

The abstract grammar for assertions is

$$\begin{aligned}
 A ::= & \text{always assert property } Q && // \text{ "always" form} \\
 & | \text{always } @ (b) \text{ assert property } P && // \text{ "always with clock" form} \\
 & | \text{initial assert property } Q && // \text{ "initial" form} \\
 & | \text{initial } @ (b) \text{ assert property } P && // \text{ "initial with clock" form}
 \end{aligned}$$

0. Preliminaries

Notation 0:

- \models_{sva} denotes the SVA relation of tight satisfaction by a finite word of an unlocked sequence.
- \models_{psl} denotes the PSL relation of tight satisfaction by a finite word of an unlocked SERE.
- \models_{psl}^c denotes the PSL relation of tight satisfaction by a finite word of a (clocked) SERE in the context of clock c .
- \models denotes the relation of satisfaction by a letter (or word of length 1) of a boolean expression in both SVA and PSL.
- \models_{sva} denotes the SVA relation of satisfaction by a word of an unlocked property or assertion
- \models_{psl} denotes the PSL relation of satisfaction by a word of an unlocked formula
- \models_{psl}^c denotes the PSL relation of satisfaction by a word of a (clocked) formula in the context of clock c .

□

Definition 0.1: A word w over Σ is called *proper* if it is of the form $w = uv$, where u is a word over $2^{\mathbf{P}}$ and v is one of the following: emptyword, \top^ω , or \perp^ω . □

0.1 Lemmas on unlocked SERES

Lemma 0.1: *Let w be a finite word over Σ . w is a clock tick of TRUE iff $w = \top^k a$, where $k \geq 0$ and $a \neq \perp$.*

Proof:

w is a clock tick of TRUE
iff $|w| > 0$ and $w^{|w|-1} \models \text{TRUE}$ and for every $0 \leq i < |w| - 1$, $w^i \models \text{FALSE}$
iff $|w| > 0$ and $w^{|w|-1} \neq \perp$ and for every $0 \leq i < |w| - 1$, $w^i = \top$
iff $[k = |w| - 1, a = w^{|w|-1}]$
 $w = \top^k a$ where $k \geq 0$ and $a \neq \perp$

□

Proposition 0.1: *Let w be a finite word over Σ and let r be an unlocked SERE. If $w \models_{\text{psl}} r$, then $w \models_{\text{psl}}^{\text{TRUE}} r$.*

Proof: By induction over the structure of r . Note that for each of the primitive unlocked SERE forms except boolean expression, the corresponding clocked SERE definition is obtained by changing \models_{psl} to \models_{psl}^c . Therefore it is enough to check the implication in the case of boolean expressions.

$w \models_{\text{psl}} b$
iff $|w| = 1$ and $w^0 \models b$
iff $w = \top^0 w^0$ and $w^0 \neq \perp$ and $w^0 \models b$
 \Rightarrow [Lemma 0.1]
 w is a clock tick of TRUE and $w^{|w|-1} \models b$
iff $w \models_{\text{psl}}^{\text{TRUE}} b$

□

Remark: The converse of the preceding proposition does not hold. For example, $\top^2 \models_{\text{psl}}^{\text{TRUE}} \text{TRUE}$, but $\top^2 \not\models_{\text{psl}} \text{TRUE}$. The converse does hold if w is a word over $2^{\mathbf{P}}$.

□

Lemma 0.2: *Let w be a finite word over Σ and let r be an unlocked SERE. Then $w \models_{\text{psl}} r[+]$ iff there exist $k > 0$ and w_1, \dots, w_k such that $w = w_1 \cdots w_k$ and $w_j \models_{\text{psl}} r$ for each $1 \leq j \leq k$.*

Proof:

$w \models_{\text{psl}} r[+]$
iff $w \models_{\text{psl}} r ; r[*]$
iff there exist w_1, u_1 such that $w = w_1 u_1$ and $w_1 \models_{\text{psl}} r$ and $u_1 \models_{\text{psl}} r[*]$

By definition,

$u_1 \models_{\text{psl}} r[*]$
iff $u_1 \models_{\text{psl}} r[*0]$ or there exist w_2, u_2 such that $|w_2| > 0$ and $u_1 = w_2 u_2$ and $w_2 \models_{\text{psl}} r$ and $u_2 \models_{\text{psl}} r[*]$
iff $|u_1| = 0$ or there exist w_2, u_2 such that $|w_2| > 0$ and $u_1 = w_2 u_2$ and $w_2 \models_{\text{psl}} r$ and $u_2 \models_{\text{psl}} r[*]$

By repeating the application of this definition to the suffix u_j and using the fact that $|w|$ bounds the number of times the suffix can be split, it follows that

$$\begin{aligned} & u_1 \equiv_{\text{psl}} r[\star] \\ \text{iff } & |u_1| = 0 \text{ or there exist } k \geq 2 \text{ and non-empty } w_2, \dots, w_k \text{ such that} \\ & u_1 = w_2 \cdots w_k \text{ and } w_j \equiv_{\text{psl}} r \text{ for each } 2 \leq j \leq k \end{aligned}$$

Therefore

$$\begin{aligned} & w \equiv_{\text{psl}} r[+] \\ \text{iff} & \\ & \text{(A):} \\ & \text{there exist } w_1, u_1 \text{ such that } w = w_1 u_1 \text{ and } w_1 \equiv_{\text{psl}} r \text{ and either } |u_1| = 0 \text{ or} \\ & \text{there exist } k \geq 2 \text{ and non-empty } w_2, \dots, w_k \text{ such that } u_1 = w_2 \cdots w_k \text{ and} \\ & w_j \equiv_{\text{psl}} r \text{ for each } 2 \leq j \leq k \end{aligned}$$

Assume (A). Letting $k = 1$ if $|u_1| = 0$, it follows that

$$\begin{aligned} & \text{(B):} \\ & \text{there exist } k > 0 \text{ and } w_1, \dots, w_k \text{ such that } w = w_1 \cdots w_k \text{ and } w_j \equiv_{\text{psl}} r \text{ for} \\ & \text{each } 1 \leq j \leq k \end{aligned}$$

Assume (B). Suppose w is empty. Then all of the w_j are empty, and, since $k > 0$, $w = w_1 \equiv_{\text{psl}} r$. In this case, (A) holds with $k = 1$ and $u_1 = 0$. Otherwise, w is non-empty, so there is at least one non-empty w_j . Discard all the empty w_j and reindex. Then (A) holds, either with $k = 1$ and $u_1 = 0$ or with $k \geq 2$. □

Lemma 0.3: *If w is a finite word over Σ and if $w \equiv_{\text{psl}} r$, where r is an unclocked SERE, then no letter of w is \perp .*

Proof: By induction over the structure of r . Write $\text{good}(w)$ to mean that no letter of w is \perp .

- $r = b$.

$$\begin{aligned} & w \equiv_{\text{psl}} b \\ \text{iff } & |w| = 1 \text{ and } w^0 \Vdash b \\ \Rightarrow & |w| = 1 \text{ and } w^0 \neq \perp \\ \Rightarrow & \text{good}(w) \end{aligned}$$

- $r = \{r_1\}$.

$$\begin{aligned} & w \equiv_{\text{psl}} \{r_1\} \\ \text{iff } & w \equiv_{\text{psl}} r_1 \\ \Rightarrow & [\text{induction}] \\ & \text{good}(w) \end{aligned}$$

- $r = r_1 ; r_2$.

$w \equiv_{\text{psl}} r_1 ; r_2$
 iff there exist u, v such that $w = uv$ and $u \equiv_{\text{psl}} r_1$ and $v \equiv_{\text{psl}} r_2$
 \Rightarrow [induction]
 there exist u, v such that $w = uv$ and $\text{good}(u)$ and $\text{good}(v)$
 $\Rightarrow \text{good}(w)$

- $r = \{r_1\} : \{r_2\}$.

$w \equiv_{\text{psl}} \{r_1\} : \{r_2\}$
 iff there exist x, y, z such that $w = xyz$ and $|y| = 1$ and $xy \equiv_{\text{psl}} r_1$ and
 $yz \equiv_{\text{psl}} r_2$
 \Rightarrow [induction]
 there exist x, y, z such that $w = xyz$ and $\text{good}(xy)$ and $\text{good}(yz)$
 $\Rightarrow \text{good}(w)$

- $r = \{r_1\} | \{r_2\}$.

$w \equiv_{\text{psl}} \{r_1\} | \{r_2\}$
 iff $w \equiv_{\text{psl}} r_1$ or $w \equiv_{\text{psl}} r_2$
 \Rightarrow [induction]
 $\text{good}(w)$ or $\text{good}(w)$
 iff $\text{good}(w)$

- $r = \{r_1\} \&\& \{r_2\}$.

$w \equiv_{\text{psl}} \{r_1\} \&\& \{r_2\}$
 iff $w \equiv_{\text{psl}} r_1$ and $w \equiv_{\text{psl}} r_2$
 \Rightarrow [induction]
 $\text{good}(w)$ and $\text{good}(w)$
 iff $\text{good}(w)$

- $r = r_1 [*0]$.

$w \equiv_{\text{psl}} r_1 [*0]$
 iff $|w| = 0$
 $\Rightarrow \text{good}(w)$

- $r = r_1 [+]$.

$w \equiv_{\text{psl}} r_1 [+]$
 iff [Lemma 0.2]
 there exist $k > 0$ and w_1, \dots, w_k such that $w = w_1 \cdots w_k$ and $w_j \equiv_{\text{psl}} r_1$
 for all $1 \leq j \leq k$
 \Rightarrow [induction]
 there exist $k > 0$ and w_1, \dots, w_k such that $w = w_1 \cdots w_k$ and $\text{good}(w_j)$
 for all $1 \leq j \leq k$
 $\Rightarrow \text{good}(w)$

□

Lemma 0.4: *Let r be an unclocked SERE and let w be a word over Σ . Then the following are equivalent:*

1. *there exists $0 \leq j < |w|$ such that $w^{0..j} \models_{\text{psl}} r$*
2. *$w \models_{\text{psl}} \{r\}!$*
3. *$w \models_{\text{psl}} !(\{r\} \mid \rightarrow \text{FALSE})$*

Proof: The equivalence of 1 and 2 is by definition.

$$\begin{aligned}
& w \models_{\text{psl}} !(\{r\} \mid \rightarrow \text{FALSE}) \\
& \text{iff } \bar{w} \not\models_{\text{psl}} \{r\} \mid \rightarrow \text{FALSE} \\
& \text{iff } \neg(\text{for every } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}} r, \bar{w}^{j..} \models_{\text{psl}} \text{FALSE}) \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}} r \text{ and } \bar{w}^{j..} \not\models_{\text{psl}} \text{FALSE} \\
& \text{iff [if } 0 \leq j < |w|, \text{ then } \bar{w}^{j..} \text{ is non-empty]} \\
& \quad \text{there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}} r \text{ and } \bar{w}^j \not\models \text{FALSE} \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}} r \text{ and } \bar{w}^j \neq \top \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}} r \text{ and } w^j \neq \perp \\
& \text{iff [if } w^{0..j} \models_{\text{psl}} r, \text{ then } w^j \neq \perp \text{ by Lemma 0.3]} \\
& \quad \text{there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}} r
\end{aligned}$$

□

Lemma 0.5: *Let b be a boolean expression and let $\ell \in \Sigma$. Then $\ell \models b$ iff $\bar{\ell} \not\models !b$*

Proof: If $\ell \in 2^{\mathbf{P}}$, then $\ell = \bar{\ell}$ and the result follows because the relation \models has the property that $\ell \models b$ iff $\ell \not\models !b$ when $\ell \in 2^{\mathbf{P}}$. If $\ell = \top$, then $\ell \models b$ and $\bar{\ell} = \perp \not\models !b$. If $\ell = \perp$, then $\ell \not\models b$ and $\bar{\ell} = \top \models !b$. □

Lemma 0.6: *Let b be a boolean expression and let w be a word over Σ . Then*

1. *$w \models_{\text{psl}} b!$ iff $w \models_{\text{psl}} \{b\}!$ iff $w \models_{\text{psl}} !(\{b\} \mid \rightarrow \text{FALSE})$.*
2. *$w \models_{\text{psl}} b$ iff $w \models_{\text{psl}} \{b\}$ iff $w \models_{\text{psl}} \{!b\} \mid \rightarrow \text{FALSE}$.*

Proof:

1. By Lemma 0.4, $w \models_{\text{psl}} \{b\}!$ iff $w \models_{\text{psl}} !(\{b\} \mid \rightarrow \text{FALSE})$.

$$\begin{aligned}
& w \models_{\text{psl}} \{b\}! \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}} b \\
& \text{iff } [w^{0..j} \models_{\text{psl}} b \text{ only if } j = 0] \\
& \quad |w| > 0 \text{ and } w^{0..0} \models_{\text{psl}} b \\
& \text{iff } |w| > 0 \text{ and } w^0 \models b \\
& \text{iff } w \models_{\text{psl}} b!
\end{aligned}$$

2. $w \models_{\text{psl}} \{\!|b|\}$ \rightarrow FALSE
iff $\bar{w} \not\models_{\text{psl}} \{\!|b|\}$ \rightarrow FALSE
iff [part 1]
 $\bar{w} \not\models_{\text{psl}} (!b)!$
iff $\neg(|\bar{w}| > 0 \text{ and } \bar{w}^0 \models !b)$
iff $|w| = 0 \text{ or } \bar{w}^0 \not\models !b$
iff [Lemma 0.5]
 $|w| = 0 \text{ or } w^0 \models b$
iff $w \models_{\text{psl}} b$

- $w \models_{\text{psl}} \{b\}$
iff for all $0 \leq j < |w|$, $w^{0..j} \top^\omega \models_{\text{psl}} \{b\}!$
iff for all $0 \leq j < |w|$, there exists $0 \leq k$ such that $(w^{0..j} \top^\omega)^{0..k} \models_{\text{psl}} b$
iff $[(w^{0..j} \top^\omega)^{0..k} \models_{\text{psl}} b \text{ only if } k = 0]$
for all $0 \leq j < |w|$, $(w^{0..j} \top^\omega)^{0..0} \models_{\text{psl}} b$
iff $|w| = 0 \text{ or } w^{0..0} \models_{\text{psl}} b$
iff $|w| = 0 \text{ or } (|w| > 0 \text{ and } w^0 \models b)$
iff $|w| = 0 \text{ or } w^0 \models b$
iff $w \models_{\text{psl}} b$

□

0.2 Lemmas on (clocked) SERES

Lemma 0.7: Let w be a finite word over Σ , let c be a boolean expression, and let r be a SERE. Then $w \models_{\text{psl}}^c r[+]$ iff there exist $k > 0$ and w_1, \dots, w_k such that $w = w_1 \cdots w_k$ and $w_j \models_{\text{psl}}^c r$ for each $1 \leq j \leq k$.

Proof: Analogous to the proof of Lemma 0.2. □

Lemma 0.8: If w is a finite word over Σ , c is a boolean expression, and $w \models_{\text{psl}}^c r$, where r is a SERE, then no letter of w is \perp .

Proof: By induction over the structure of r . Write $\text{good}(w)$ to mean that no letter of w is \perp .

- $r = b$.

- $w \models_{\text{psl}}^c b$
iff w is a clock tick of c and $w^{|w|-1} \models b$
iff $|w| > 0$, $w^j \models !c$ for all $0 \leq j < |w| - 1$, and $w^{|w|-1} \models c$ and $w^{|w|-1} \models b$
 \Rightarrow [each letter of w must satisfy a boolean expression and so cannot be \perp]
 $\text{good}(w)$

- $r = \{r_1\}$.

- $w \models_{\text{psl}}^c \{r_1\}$
iff $w \models_{\text{psl}}^c r_1$
 \Rightarrow [induction]

$good(w)$

- $r = r_1 ; r_2$.

$w \equiv_{\text{psl}}^c r_1 ; r_2$

iff there exist u, v such that $w = uv$ and $u \equiv_{\text{psl}}^c r_1$ and $v \equiv_{\text{psl}}^c r_2$

\Rightarrow [induction]

there exist u, v such that $w = uv$ and $good(u)$ and $good(v)$

$\Rightarrow good(w)$

- $r = \{r_1\} : \{r_2\}$.

$w \equiv_{\text{psl}}^c \{r_1\} : \{r_2\}$

iff there exist x, y, z such that $w = xyz$ and $|y| = 1$ and $xy \equiv_{\text{psl}}^c r_1$ and

$yz \equiv_{\text{psl}}^c r_2$

\Rightarrow [induction]

there exist x, y, z such that $w = xyz$ and $good(xy)$ and $good(yz)$

$\Rightarrow good(w)$

- $r = \{r_1\} | \{r_2\}$.

$w \equiv_{\text{psl}}^c \{r_1\} | \{r_2\}$

iff $w \equiv_{\text{psl}}^c r_1$ or $w \equiv_{\text{psl}}^c r_2$

\Rightarrow [induction]

$good(w)$ or $good(w)$

iff $good(w)$

- $r = \{r_1\} \&\& \{r_2\}$.

$w \equiv_{\text{psl}}^c \{r_1\} \&\& \{r_2\}$

iff $w \equiv_{\text{psl}}^c r_1$ and $w \equiv_{\text{psl}}^c r_2$

\Rightarrow [induction]

$good(w)$ and $good(w)$

iff $good(w)$

- $r = r_1 [*0]$.

$w \equiv_{\text{psl}}^c r_1 [*0]$

iff $|w| = 0$

$\Rightarrow good(w)$

- $r = r_1 [+]$.

$w \models_{\text{psl}}^c r_1 [+]$
 iff [Lemma 0.7]
 there exist $k > 0$ and w_1, \dots, w_k such that $w = w_1 \cdots w_k$ and $w_j \models_{\text{psl}}^c r_1$
 for all $1 \leq j \leq k$
 \Rightarrow [induction]
 there exist $k > 0$ and w_1, \dots, w_k such that $w = w_1 \cdots w_k$ and $\text{good}(w_j)$
 for all $1 \leq j \leq k$
 $\Rightarrow \text{good}(w)$

• $r = r_1 @ c_1$.

$w \models_{\text{psl}}^c r_1 @ c_1$
 iff $w \models_{\text{psl}}^{c_1} r_1$
 \Rightarrow [induction]
 $\text{good}(w)$

□

Lemma 0.9: *Let r be a SERE, let c be a boolean expression, and let w be a word over Σ . Then the following are equivalent:*

1. *there exists $0 \leq j < |w|$ such that $w^{0..j} \models_{\text{psl}}^c r$*
2. $w \models_{\text{psl}}^c \{r\}!$
3. $w \models_{\text{psl}}^c !(\{r\} \mid \rightarrow \text{FALSE} @ \text{TRUE})$

Proof: The equivalence of 1 and 2 is by definition.

$w \models_{\text{psl}}^c !(\{r\} \mid \rightarrow \text{FALSE} @ \text{TRUE})$
 iff $\bar{w} \not\models_{\text{psl}}^c \{r\} \mid \rightarrow \text{FALSE} @ \text{TRUE}$
 iff $\neg(\text{for every } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^c r, \bar{w}^{j..} \models_{\text{psl}}^c \text{FALSE} @ \text{TRUE})$
 iff $\neg(\text{for every } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^c r, \bar{w}^{j..} \models_{\text{psl}}^{\text{TRUE}} \text{FALSE})$
 iff there exists $0 \leq j < |w|$ such that $w^{0..j} \models_{\text{psl}}^c r$ and $\neg(\bar{w}^{j..} \models_{\text{psl}}^{\text{TRUE}} \text{FALSE})$
 iff there exists $0 \leq j < |w|$ such that $w^{0..j} \models_{\text{psl}}^c r$ and $\neg(\text{for all } j \leq k < |w|$
 such that $w^{j..k}$ is a clock tick of TRUE, $\bar{w}^k \models \text{FALSE})$
 iff there exists $0 \leq j < |w|$ such that $w^{0..j} \models_{\text{psl}}^c r$ and there exists $j \leq k < |w|$
 such that $w^{j..k}$ is a clock tick of TRUE and $\bar{w}^k \not\models \text{FALSE}$
 iff [if $w^{j..k}$ is a clock tick of TRUE, then $w^k \models \text{TRUE}$, hence $w^k \neq \perp$, hence
 $\bar{w}^k \neq \top$, hence $\bar{w}^k \not\models \text{FALSE}$]
 there exists $0 \leq j < |w|$ such that $w^{0..j} \models_{\text{psl}}^c r$ and there exists $j \leq k < |w|$
 such that $w^{j..k}$ is a clock tick of TRUE
 iff [if $w^{0..j} \models_{\text{psl}}^c r$, then $w^j \neq \perp$, so $w^{j..j}$ is a clock tick of TRUE]
 there exists $0 \leq j < |w|$ such that $w^{0..j} \models_{\text{psl}}^c r$

□

Lemma 0.10: *Let r_1, r_2 be SERES, let c be a boolean expression, and let w be a word over Σ . Then the following are equivalent:*

1. for every $0 \leq j < |w|$ such that $\bar{w}^{0..j} \models_{\text{psl}}^c r_1$, there exists $j \leq k < |w|$ such that $w^{j..k} \models_{\text{psl}}^c r_2$
2. $w \models_{\text{psl}}^c \{r_1\} \mid \rightarrow \{r_2\}!$
3. $w \models_{\text{psl}}^c \{r_1\} \mid \rightarrow !(\{r_2\} \mid \rightarrow \text{FALSE@TRUE})$

Proof: Immediate from Lemma 0.9 and the definitions. \square

Lemma 0.11: *If w is a non-empty finite word over Σ , c is a boolean expression, and $w \models_{\text{psl}}^c r$, where r is an unlocked SERE, then $w^{|w|-1} \models c$.*

Proof: By induction over the structure of r . Let $I = |w| - 1$.

- $r = b$.

$$\begin{aligned}
& w \models_{\text{psl}}^c b \\
& \text{iff } w \text{ is a clock tick of } c \text{ and } w^{|w|-1} \models b \\
& \text{iff } |w| > 0, w^j \models !c \text{ for all } 0 \leq j < |w| - 1, \text{ and } w^{|w|-1} \models c \text{ and } w^{|w|-1} \models b \\
& \Rightarrow w^I \models c
\end{aligned}$$

- $r = \{r_1\}$.

$$\begin{aligned}
& w \models_{\text{psl}}^c \{r_1\} \\
& \text{iff } w \models_{\text{psl}}^c r_1 \\
& \Rightarrow [\text{induction}] \\
& \quad w^I \models c
\end{aligned}$$

- $r = r_1 ; r_2$.

$$\begin{aligned}
& w \models_{\text{psl}}^c r_1 ; r_2 \\
& \text{iff there exist } u, v \text{ such that } w = uv \text{ and } u \models_{\text{psl}}^c r_1 \text{ and } v \models_{\text{psl}}^c r_2 \\
& \Rightarrow [\text{induction}] \\
& \quad w = uv \text{ and if } u \text{ is non-empty then } u^{|u|-1} \models c \text{ and if } v \text{ is non-empty then } \\
& \quad v^{|v|-1} \models c \\
& \Rightarrow [w = uv \text{ is non-empty; if } |v| > 0 \text{ then } w^I = v^{|v|-1}; \text{ otherwise } w^I = u^{|u|-1}] \\
& \quad w^I \models c
\end{aligned}$$

- $r = \{r_1\} : \{r_2\}$.

$$\begin{aligned}
& w \models_{\text{psl}}^c \{r_1\} : \{r_2\} \\
& \text{iff there exist } x, y, z \text{ such that } w = xyz \text{ and } |y| = 1 \text{ and } xy \models_{\text{psl}}^c r_1 \text{ and } \\
& \quad yz \models_{\text{psl}}^c r_2 \\
& \Rightarrow [\text{induction}] \\
& \quad w = xyz \text{ and } yz^{|yz|-1} \models c \\
& \Rightarrow [w^I = yz^{|yz|-1}] \\
& \quad w^I \models c
\end{aligned}$$

- $r = \{r_1\} \mid \{r_2\}$.

$$\begin{aligned}
& w \equiv_{\text{psl}}^c \{r_1\} \mid \{r_2\} \\
& \text{iff } w \equiv_{\text{psl}}^c r_1 \text{ or } w \equiv_{\text{psl}}^c r_2 \\
& \Rightarrow [\text{induction}] \\
& \quad w^I \models c \text{ or } w^I \models c \\
& \text{iff } w^I \models c
\end{aligned}$$

- $r = \{r_1\} \&\& \{r_2\}$.

$$\begin{aligned}
& w \equiv_{\text{psl}}^c \{r_1\} \&\& \{r_2\} \\
& \text{iff } w \equiv_{\text{psl}}^c r_1 \text{ and } w \equiv_{\text{psl}}^c r_2 \\
& \Rightarrow [\text{induction}] \\
& \quad w^I \models c \text{ and } w^I \models c \\
& \text{iff } w^I \models c
\end{aligned}$$

- $r = r_1 [*0]$.

$$\begin{aligned}
& w \equiv_{\text{psl}}^c r_1 [*0] \\
& \text{iff } |w| = 0 \\
& \text{iff } [w \text{ is non-empty}] \\
& \quad \mathbb{F}
\end{aligned}$$

- $r = r_1 [+]$.

$$\begin{aligned}
& w \equiv_{\text{psl}}^c r_1 [+] \\
& \text{iff } [\text{Lemma 0.7}] \\
& \quad \text{there exist } k > 0 \text{ and } w_1, \dots, w_k \text{ such that } w = w_1 \cdots w_k \text{ and } w_j \equiv_{\text{psl}}^c r_1 \text{ for} \\
& \quad \text{all } 1 \leq j \leq k \\
& \text{iff } [\text{throw away unnecessary empty } w_j \text{ and reindex}] \\
& \quad \text{there exist } k > 0 \text{ and non-empty } w_1, \dots, w_k \text{ such that } w = w_1 \cdots w_k \text{ and} \\
& \quad w_j \equiv_{\text{psl}}^c r_1 \text{ for all } 1 \leq j \leq k \\
& \Rightarrow [\text{induction}] \\
& \quad \text{there exist } k > 0 \text{ and non-empty } w_1, \dots, w_k \text{ such that } w = w_1 \cdots w_k \text{ and} \\
& \quad w_j^{|w_j|^{-1}} \models c \text{ all } 1 \leq j \leq k \\
& \Rightarrow [w^I = w_k^{|w_k|^{-1}}] \\
& \quad w^I \models c
\end{aligned}$$

□

Lemma 0.12: *Let r be an unclocked SERE, let c be a boolean expression, and let w be a word over Σ . Then the following are equivalent:*

1. *there exists $0 \leq j < |w|$ such that $w^{0..j} \equiv_{\text{psl}}^c r$*

2. $w \models_{\text{psl}}^c \{r\}!$
3. $w \models_{\text{psl}}^c !(\{r\} \mid \rightarrow \text{FALSE})$

Proof: The equivalence of 1 and 2 is by definition.

$$\begin{aligned}
& w \models_{\text{psl}}^c !(\{r\} \mid \rightarrow \text{FALSE}) \\
& \text{iff } \bar{w} \not\models_{\text{psl}}^c \{r\} \mid \rightarrow \text{FALSE} \\
& \text{iff } \neg(\text{for every } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^c r, \bar{w}^{j..} \models_{\text{psl}}^c \text{FALSE}) \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^c r \text{ and } \bar{w}^{j..} \not\models_{\text{psl}}^c \text{FALSE} \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^c r \text{ and } \neg(\text{for all } j \leq k < |w| \\
& \quad \text{such that } w^{j..k} \text{ is a clock tick of } c, \text{ then } \bar{w}^k \models \text{FALSE}) \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^c r \text{ and there exists } j \leq k < |w| \\
& \quad \text{such that } w^{j..k} \text{ is a clock tick of } c \text{ and } \bar{w}^k \not\models \text{FALSE} \\
& \text{iff [if } w^{j..k} \text{ is a clock tick of } c, \text{ then } w^k \models c, \text{ hence } w^k \neq \perp, \text{ hence } \bar{w}^k \neq \top, \\
& \quad \text{hence } \bar{w}^k \not\models \text{FALSE}] \\
& \quad \text{there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^c r \text{ and there exists } j \leq k < |w| \\
& \quad \text{such that } w^{j..k} \text{ is a clock tick of } c \\
& \text{iff [if } w^{0..j} \models_{\text{psl}}^c r, \text{ then, by Lemma 0.11, } w^j \models c, \text{ hence } w^{j..j} \text{ is a clock tick of} \\
& \quad c] \\
& \quad \text{there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^c r
\end{aligned}$$

□

Lemma 0.13 (Duality of Boolean Formulas): *Let b, c be boolean expressions and let w be a word over Σ . Use the following notation to eliminate ambiguity:*

- $[!b]$ denotes the boolean expression negation of b ;
- $[!b]!$ denotes the strong boolean formula built from $[!b]$;
- $!([!b]!)$ denotes the formula negation of the strong boolean formula $[!b]!$;
- $!(b!)$ denotes the formula negation of the strong boolean formula $b!$.

Then

1. $w \models_{\text{psl}}^c !([!b]!) \text{ iff } w \models_{\text{psl}}^c b$
2. $w \models_{\text{psl}}^c !(b!) \text{ iff } w \models_{\text{psl}}^c [!b]$

Proof: Note that 2 follows from 1 by negating the boolean expression. Here is the proof of 1:

$$\begin{aligned}
& w \models_{\text{psl}}^c !([!b]!) \\
& \text{iff } \bar{w} \not\models_{\text{psl}}^c [!b]! \\
& \text{iff } \neg(\text{there exists } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \text{ is a clock tick of } c \text{ and } \bar{w}^j \models !b) \\
& \text{iff for all } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \text{ is a clock tick of } c, \bar{w}^j \not\models !b \\
& \text{iff [Lemma 0.5]} \\
& \quad \text{for all } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \text{ is a clock tick of } c, w^j \models b \\
& \text{iff } w \models_{\text{psl}}^c b
\end{aligned}$$

□

Lemma 0.14: *Let b, c be boolean expressions and let w be a word over Σ . Then*

1. $w \models_{\text{psl}}^c b!$ iff $w \models_{\text{psl}}^c \{b\}!$ iff $w \models_{\text{psl}}^c !(\{b\} \mid \rightarrow \text{FALSE})$.
2. $w \models_{\text{psl}}^c b$ iff $w \models_{\text{psl}}^c \{b\}$ iff $w \models_{\text{psl}}^c \{!b\} \mid \rightarrow \text{FALSE}$.

Proof: By Lemma 0.12, $w \models_{\text{psl}}^c \{b\}!$ iff $w \models_{\text{psl}}^c !(\{b\} \mid \rightarrow \text{FALSE})$.

$$\begin{aligned}
& w \models_{\text{psl}}^c \{b\}! \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^c b \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \text{ is a clock tick of } c \text{ and } w^j \models b \\
& \text{iff } w \models_{\text{psl}}^c b!
\end{aligned}$$

This proves 1.

$$\begin{aligned}
& w \models_{\text{psl}}^c \{!b\} \mid \rightarrow \text{FALSE} \\
& \text{iff } \bar{w} \not\models_{\text{psl}}^c !(\{!b\} \mid \rightarrow \text{FALSE}) \\
& \text{iff [part 1, notation from Lemma 0.13]} \\
& \quad \bar{w} \not\models_{\text{psl}}^c [!b]! \\
& \text{iff } \neg(\text{there exists } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \text{ is a clock tick of } c \text{ and } \bar{w}^j \models !b) \\
& \text{iff for all } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \text{ is a clock tick of } c, \bar{w}^j \not\models !b \\
& \text{iff [Lemma 0.5]} \\
& \quad \text{for all } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \text{ is a clock tick of } c, w^j \models b \\
& \text{iff } w \models_{\text{psl}}^c b
\end{aligned}$$

Also

$$\begin{aligned}
& w \models_{\text{psl}}^c \{b\} \\
& \text{iff for all } 0 \leq j < |w|, w^{0..j} \top \omega \models_{\text{psl}}^c \{b\}! \\
& \text{iff for all } 0 \leq j < |w|, \text{ there exists } 0 \leq k \text{ such that } (w^{0..j} \top \omega)^{0..k} \models_{\text{psl}}^c b \\
& \text{iff} \\
& \quad \text{(A):} \\
& \quad \text{for all } 0 \leq j < |w|, \text{ there exists } 0 \leq k \text{ such that } (w^{0..j} \top \omega)^{0..k} \text{ is a clock tick} \\
& \quad \text{of } c \text{ and } (w^{0..j} \top \omega)^k \models b
\end{aligned}$$

and

$$\begin{aligned}
& w \models_{\text{psl}}^c b \\
& \text{iff} \\
& \quad \text{(B):} \\
& \quad \text{for all } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \text{ is a clock tick of } c, w^j \models b
\end{aligned}$$

Assume (A). Let $0 \leq j < |w|$ be such that $\bar{w}^{0..j}$ is a clock tick of c . By (A), there exists $0 \leq k$ such that $(w^{0..j} \top \omega)^{0..k}$ is a clock tick of c and $(w^{0..j} \top \omega)^k \models b$. In order to prove (B), it suffices to show that $k = j$, since then it follows that $w^j = (w^{0..j} \top \omega)^k \models b$. Suppose that $k < j$. Then $(w^{0..j} \top \omega)^{0..k} = w^{0..k}$ is a clock tick of c , and so $w^k \models c$. Since $\bar{w}^{0..j}$ is a clock tick of c , $\bar{w}^k \models !c$, so by Lemma 0.5, $w^k \not\models c$, a contradiction. Suppose that $k > j$. Then $(w^{0..j} \top \omega)^{0..k} = w^{0..j} \top \omega^{k-j}$

is a clock tick of c . Therefore, $w^j \Vdash !c$. Since $\bar{w}^{0..j}$ is a clock tick of c , $\bar{w}^j \Vdash c$, so by Lemma 0.5, $w^j \not\Vdash !c$, a contradiction.

Now assume (B). Let

$$I = \{0 \leq i < |w| : w^i \notin 2^{\mathbf{P}} \text{ or } w^i \Vdash c\}.$$

Suppose I is empty. Then, for all $0 \leq i < |w|$, $w^i \in 2^{\mathbf{P}}$ and $w^i \Vdash !c$. Let $0 \leq j < |w|$. Then $w^{0..j}\top$ is a clock tick of c and $(w^{0..j}\top)^{j+1} = \top \Vdash b$. This proves (A) when I is empty. Suppose now that I is non-empty. Let $m = \min I$. Then $m < |w|$ and for all $0 \leq i < m$, $w^i \in 2^{\mathbf{P}}$ and $w^i \Vdash !c$. The following are the possible cases for w^m :

- $w^m = \perp$. Then $\bar{w}^{0..m}$ is a clock tick of c , so by (B) $w^m \Vdash b$, a contradiction.
- $w^m = \top$. Then $w^{0..m}$ is a clock tick of c and $w^m \Vdash b$.
- $w^m \in 2^{\mathbf{P}}$ and $w^m \Vdash c$. Then $w^{0..m}$ is a clock tick of c and $\bar{w}^{0..m} = w^{0..m}$. By (B), $w^m \Vdash b$.

Therefore, $w^{0..m}$ is a clock tick of c and $w^m \Vdash b$. Let $0 \leq j < |w|$. If $j \geq m$, then $(w^{0..j}\top^\omega)^{0..m} = w^{0..m}$. If $j < m$, then $(w^{0..j}\top^\omega)^{0..j+1} = w^{0..j}\top$, which is a clock tick of c , and $(w^{0..j}\top^\omega)^{j+1} = \top \Vdash b$. This proves (A) when I is non-empty and completes the proof of 2. □

Lemma 0.15: *Let b, c be boolean expressions and let w be a non-empty word over Σ such that $\bar{w}^0 \Vdash c$. Then $w \Vdash_{\text{psl}}^c b$ iff $w \Vdash_{\text{psl}}^c b!$.*

Proof: Assume that $w \Vdash_{\text{psl}}^c b$. Since $\bar{w}^0 \Vdash c$, $\bar{w}^{0..0}$ is a clock tick of c , hence $w^0 \Vdash b$. Then $\bar{w}^0 \neq \perp$ and $w^0 \neq \perp$, hence $w^0 \in 2^{\mathbf{P}}$. Therefore, $w^{0..0}$ is a clock tick of c , and so $w \Vdash_{\text{psl}}^c b!$.

Assume now that $w \Vdash_{\text{psl}}^c b!$. Then there exists $0 \leq j < |w|$ such that $w^{0..j}$ is a clock tick of c and $w^j \Vdash b$. Since $\bar{w}^0 \Vdash c$, Lemma 0.5 gives $w^0 \not\Vdash !c$. Therefore, $j = 0$ and so $w^0 \Vdash c$ and $w^0 \Vdash b$. Let $0 \leq i < |w|$ be such that $\bar{w}^{0..i}$ is a clock tick of c . Suppose that $0 < i$. Then $\bar{w}^0 \Vdash !c$, so, by Lemma 0.5, $w^0 \not\Vdash c$, a contradiction. Therefore $i = 0$. Since $w^0 \Vdash b$, this proves that $w \Vdash_{\text{psl}}^c b$. □

Lemma 0.16: *Let b, c be boolean expressions and let w be a non-empty word over Σ .*

1. *If $w^0 = \top$, then $w \Vdash_{\text{psl}}^c b$ and $w \Vdash_{\text{psl}}^c b!$.*
2. *If $w^0 = \perp$, then $w \not\Vdash_{\text{psl}}^c b$ and $w \not\Vdash_{\text{psl}}^c b!$.*
3. *If $w^0 \in 2^{\mathbf{P}}$ and $w^0 \Vdash c$, then $w \Vdash_{\text{psl}}^c b$ iff $w \Vdash_{\text{psl}}^c b!$ iff $w^0 \Vdash b$.*

Proof: Assume $w^0 = \top$. Then $w^{0..0}$ is a clock tick of c and $w^0 \Vdash b$, so $w \Vdash_{\text{psl}}^c b!$. Also, $\bar{w}^0 = \perp$, so there does not exist $0 \leq i < |w|$ such that $\bar{w}^{0..i}$ is a clock tick of c . Therefore, $w \Vdash_{\text{psl}}^c b$ holds vacuously. This proves 1.

Assume now that $w^0 = \perp$. Then there does not exist $0 \leq i < |w|$ such that $w^{0..i}$ is a clock tick of c , so $w \not\models_{\text{psl}}^c b!$. Also, $\bar{w}^0 = \top$, so $\bar{w}^{0..0}$ is a clock tick of c . Since $w^0 \not\models b$, $w \not\models_{\text{psl}}^c b$. This proves 2.

Assume now that $w^0 \in 2^{\mathbf{P}}$ and $w^0 \models c$. Then $w^0 = \bar{w}^0$, so by Lemma 0.15, $w \models_{\text{psl}}^c b$ iff $w \models_{\text{psl}}^c b!$.

- $w \models_{\text{psl}}^c b!$
- iff there exists $0 \leq i < |w|$ such that $w^{0..i}$ is a clock tick of c and $w^i \models b$
- iff [since $w^0 \in 2^{\mathbf{P}}$ and $w^0 \models c$, $w^{0..0}$ is a clock tick of c and $w^{0..i}$ is not a clock tick of c if $i > 0$]
- $w^0 \models b$

This proves 3. □

1. Mapping unlocked SVA sequences to PSL unlocked SERES

Definition 1: Let b be a boolean expression, and let R, R_1, R_2 be unlocked SVA sequences.

- $\mathfrak{M}(b) = b$
- $\mathfrak{M}((R)) = \{\mathfrak{M}(R)\}$
- $\mathfrak{M}((R_1 \#\#1 R_2)) = \{\mathfrak{M}(R_1) ; \mathfrak{M}(R_2)\}$
- $\mathfrak{M}((R_1 \#\#0 R_2)) = \{\{\mathfrak{M}(R_1)\} : \{\mathfrak{M}(R_2)\}\}$
- $\mathfrak{M}((R_1 \text{ or } R_2)) = \{\{\mathfrak{M}(R_1)\} \mid \{\mathfrak{M}(R_2)\}\}$
- $\mathfrak{M}((R_1 \text{ intersect } R_2)) = \{\{\mathfrak{M}(R_1)\} \&\& \{\mathfrak{M}(R_2)\}\}$
- $\mathfrak{M}(R[*0]) = \mathfrak{M}(R)[*0]$
- $\mathfrak{M}(R[*1:\$]) = \mathfrak{M}(R)[+]$

□

Proposition 1.1: Let R be an unlocked SVA sequence and let w be a finite word over Σ . Then $w \models_{\text{sva}} R$ iff $w \models_{\text{psl}} \mathfrak{M}(R)$.

Proof: By induction over the structure of R .

- $R = b$.

- $w \models_{\text{sva}} b$
- iff $|w| = 1$ and $w^0 \models b$
- iff $|w| = 1$ and $w^0 \models \mathfrak{M}(b)$
- iff $w \models_{\text{psl}} \mathfrak{M}(b)$

- $R = (R_1)$.

$w \models_{\text{sva}} (R_1)$
 iff $w \models_{\text{sva}} R_1$
 iff [induction]
 $w \models_{\text{psl}} \mathfrak{M}(R_1)$
 iff $w \models_{\text{psl}} \{\mathfrak{M}(R_1)\}$
 iff $w \models_{\text{psl}} \mathfrak{M}((R_1))$

- $R = (R_1 \#\#1 R_2)$.

$w \models_{\text{sva}} (R_1 \#\#1 R_2)$
 iff there exist x, y such that $w = xy$ and $x \models_{\text{sva}} R_1$ and $y \models_{\text{sva}} R_2$
 iff [induction]
 there exist x, y such that $w = xy$ and $x \models_{\text{psl}} \mathfrak{M}(R_1)$ and $y \models_{\text{psl}} \mathfrak{M}(R_2)$
 iff $w \models_{\text{psl}} \mathfrak{M}(R_1) ; \mathfrak{M}(R_2)$
 iff $w \models_{\text{psl}} \{\mathfrak{M}(R_1) ; \mathfrak{M}(R_2)\}$
 iff $w \models_{\text{psl}} \mathfrak{M}((R_1 \#\#1 R_2))$

- $R = (R_1 \#\#0 R_2)$.

$w \models_{\text{sva}} (R_1 \#\#0 R_2)$
 iff there exist x, y, z such that $w = xyz$ and $|y| = 1$ and $xy \models_{\text{sva}} R_1$
 and $yz \models_{\text{sva}} R_2$
 iff [induction]
 there exist x, y such that $w = xyz$ and $|y| = 1$ and $xy \models_{\text{psl}} \mathfrak{M}(R_1)$ and
 $yz \models_{\text{psl}} \mathfrak{M}(R_2)$
 iff $w \models_{\text{psl}} \{\mathfrak{M}(R_1)\} : \{\mathfrak{M}(R_2)\}$
 iff $w \models_{\text{psl}} \{\{\mathfrak{M}(R_1)\} : \{\mathfrak{M}(R_2)\}\}$
 iff $w \models_{\text{psl}} \mathfrak{M}((R_1 \#\#0 R_2))$

- $R = (R_1 \text{ or } R_2)$.

$w \models_{\text{sva}} (R_1 \text{ or } R_2)$
 iff $w \models_{\text{sva}} R_1$ or $w \models_{\text{sva}} R_2$
 iff [induction]
 $w \models_{\text{psl}} \mathfrak{M}(R_1)$ or $w \models_{\text{psl}} \mathfrak{M}(R_2)$
 iff $w \models_{\text{psl}} \{\mathfrak{M}(R_1)\} \mid \{\mathfrak{M}(R_2)\}$
 iff $w \models_{\text{psl}} \{\{\mathfrak{M}(R_1)\} \mid \{\mathfrak{M}(R_2)\}\}$
 iff $w \models_{\text{psl}} \mathfrak{M}((R_1 \text{ or } R_2))$

- $R = (R_1 \text{ intersect } R_2)$.

$w \models_{\text{sva}} (R_1 \text{ intersect } R_2)$
 iff $w \models_{\text{sva}} R_1$ and $w \models_{\text{sva}} R_2$

iff [induction]
 $w \models_{\text{psl}} \mathfrak{M}(R_1)$ and $w \models_{\text{psl}} \mathfrak{M}(R_2)$
 iff $w \models_{\text{psl}} \{\mathfrak{M}(R_1)\} \&\& \{\mathfrak{M}(R_2)\}$
 iff $w \models_{\text{psl}} \{\{\mathfrak{M}(R_1)\} \&\& \{\mathfrak{M}(R_2)\}\}$
 iff $w \models_{\text{psl}} \mathfrak{M}((R_1 \text{ intersect } R_2))$

- $R = R_1 [*0]$.

$w \models_{\text{sva}} R_1 [*0]$
 iff $|w| = 0$
 iff $w \models_{\text{psl}} \mathfrak{M}(R_1) [*0]$
 iff $w \models_{\text{psl}} \mathfrak{M}(R_1 [*0])$

- $R = R_1 [*1:\$]$.

$w \models_{\text{sva}} R_1 [*1:\$]$
 iff there exist w_1, \dots, w_j , $j \geq 1$, such that $w = w_1 \cdots w_j$ and for each i such that $1 \leq i \leq j$, $w_i \models_{\text{sva}} R_1$
 iff [induction]
 there exist w_1, \dots, w_j , $j \geq 1$, such that $w = w_1 \cdots w_j$ and for each i such that $1 \leq i \leq j$, $w_i \models_{\text{psl}} \mathfrak{M}(R_1)$
 iff [Lemma 0.2]
 $w \models_{\text{psl}} \mathfrak{M}(R_1) [+]$
 iff $w \models_{\text{psl}} \mathfrak{M}(R_1 [*1:\$])$

□

2. Mapping clocked SVA sequences to PSL clocked SERES

Notation: If S is a clocked SVA sequence, let $\langle S \rangle$ denote the unclocked SVA sequence that results from S by applying the SVA clock rewrite rules. □

Proposition 2.1: Let R be an unclocked SVA sequence, and let w be a finite word over Σ . Then $w \models_{\text{sva}} \langle @ (c) R \rangle$ iff $w \models_{\text{psl}}^c \mathfrak{M}(R)$.

Proof: By induction over the structure of R .

- $R = b$.

$w \models_{\text{sva}} \langle @ (c) b \rangle$
 iff $w \models_{\text{sva}} (!c[*0:\$] \#\#1 c \&\& b)$
 iff $w \models_{\text{sva}} ((!c[*0] \text{ or } !c[*1:\$]) \#\#1 c \&\& b)$
 iff there exist u, v such that $w = uv$ and $u \models_{\text{sva}} (!c[*0] \text{ or } !c[*1:\$])$ and $v \models_{\text{sva}} c \&\& b$
 iff there exist u, v such that $w = uv$ and $(u \models_{\text{sva}} !c[*0] \text{ or } u \models_{\text{sva}} !c[*1:\$])$

- and $|v| = 1$ and $v \models c \ \&\& \ b$
- iff there exist u, v such that $w = uv$ and ($|u| = 0$ or there exist $k \geq 1$ and u_1, \dots, u_k such that $u = u_1 \cdots u_k$ and for all $0 \leq i < k$, $u_i \models_{\text{sva}} !c$) and $|v| = 1$ and $v \models c$ and $v \models b$
- iff there exist u, v such that $w = uv$ and ($|u| = 0$ or there exist $k \geq 1$ and u_1, \dots, u_k such that $u = u_1 \cdots u_k$ and for all $0 \leq i < k$, $|u_i| = 1$ and $u_i \models !c$) and $|v| = 1$ and $v \models c$ and $v \models b$
- iff $|w| \geq 1$ and for every i such that $0 \leq i < |w| - 1$, $w^i \models !c$ and $w^{|w|-1} \models c$ and $w^{|w|-1} \models b$
- iff $w \models_{\text{psl}}^c b$
- iff $w \models_{\text{psl}}^c \mathfrak{M}(b)$

- $R = (R_1)$.

- $w \models_{\text{sva}} \langle \mathfrak{Q}(c) (R_1) \rangle$
- iff $w \models_{\text{sva}} \langle \mathfrak{Q}(c) R_1 \rangle$
- iff [induction]
- $w \models_{\text{psl}}^c \mathfrak{M}(R_1)$
- iff $w \models_{\text{psl}}^c \{\mathfrak{M}(R_1)\}$
- iff $w \models_{\text{psl}}^c \mathfrak{M}((R_1))$

- $R = (R_1 \ \#\#1 \ R_2)$.

- $w \models_{\text{sva}} \langle \mathfrak{Q}(c) (R_1 \ \#\#1 \ R_2) \rangle$
- iff $w \models_{\text{sva}} \langle \langle \mathfrak{Q}(c) R_1 \rangle \ \#\#1 \ \langle \mathfrak{Q}(c) R_2 \rangle \rangle$
- iff there exist x, y such that $w = xy$ and $x \models_{\text{sva}} \langle \mathfrak{Q}(c) R_1 \rangle$ and $y \models_{\text{sva}} \langle \mathfrak{Q}(c) R_2 \rangle$
- iff [induction]
- there exist x, y such that $w = xy$ and $x \models_{\text{psl}}^c \mathfrak{M}(R_1)$ and $y \models_{\text{psl}}^c \mathfrak{M}(R_2)$
- iff $w \models_{\text{psl}}^c \mathfrak{M}(R_1) ; \mathfrak{M}(R_2)$
- iff $w \models_{\text{psl}}^c \{\mathfrak{M}(R_1) ; \mathfrak{M}(R_2)\}$
- iff $w \models_{\text{psl}}^c \mathfrak{M}((R_1 \ \#\#1 \ R_2))$

- $R = (R_1 \ \#\#0 \ R_2)$.

- $w \models_{\text{sva}} \langle \mathfrak{Q}(c) (R_1 \ \#\#0 \ R_2) \rangle$
- iff $w \models_{\text{sva}} \langle \langle \mathfrak{Q}(c) R_1 \rangle \ \#\#0 \ \langle \mathfrak{Q}(c) R_2 \rangle \rangle$
- iff there exist x, y, z such that $w = xyz$ and $|y| = 1$ and $xy \models_{\text{sva}} \langle \mathfrak{Q}(c) R_1 \rangle$ and $yz \models_{\text{sva}} \langle \mathfrak{Q}(c) R_2 \rangle$
- iff [induction]
- there exist x, y, z such that $w = xyz$ and $|y| = 1$ and $xy \models_{\text{psl}}^c \mathfrak{M}(R_1)$ and $yz \models_{\text{psl}}^c \mathfrak{M}(R_2)$
- iff $w \models_{\text{psl}}^c \{\mathfrak{M}(R_1)\} : \{\mathfrak{M}(R_2)\}$
- iff $w \models_{\text{psl}}^c \{\{\mathfrak{M}(R_1)\} : \{\mathfrak{M}(R_2)\}\}$
- iff $w \models_{\text{psl}}^c \mathfrak{M}((R_1 \ \#\#0 \ R_2))$

- $R = (R_1 \text{ or } R_2)$.

$$\begin{aligned}
& w \models_{\text{sva}} \langle \mathcal{Q}(c) (R_1 \text{ or } R_2) \rangle \\
& \text{iff } w \models_{\text{sva}} (\langle \mathcal{Q}(c) R_1 \rangle \text{ or } \langle \mathcal{Q}(c) R_2 \rangle) \\
& \text{iff } w \models_{\text{sva}} \langle \mathcal{Q}(c) R_1 \rangle \text{ or } w \models_{\text{sva}} \langle \mathcal{Q}(c) R_2 \rangle \\
& \text{iff [induction]} \\
& \quad w \models_{\text{psl}}^c \mathfrak{M}(R_1) \text{ or } w \models_{\text{psl}}^c \mathfrak{M}(R_2) \\
& \text{iff } w \models_{\text{psl}}^c \{\mathfrak{M}(R_1)\} \mid \{\mathfrak{M}(R_2)\} \\
& \text{iff } w \models_{\text{psl}}^c \{\{\mathfrak{M}(R_1)\} \mid \{\mathfrak{M}(R_2)\}\} \\
& \text{iff } w \models_{\text{psl}}^c \mathfrak{M}((R_1 \text{ or } R_2))
\end{aligned}$$

- $R = (R_1 \text{ intersect } R_2)$.

$$\begin{aligned}
& w \models_{\text{sva}} \langle \mathcal{Q}(c) (R_1 \text{ intersect } R_2) \rangle \\
& \text{iff } w \models_{\text{sva}} (\langle \mathcal{Q}(c) R_1 \rangle \text{ intersect } \langle \mathcal{Q}(c) R_2 \rangle) \\
& \text{iff } w \models_{\text{sva}} \langle \mathcal{Q}(c) R_1 \rangle \text{ and } w \models_{\text{sva}} \langle \mathcal{Q}(c) R_2 \rangle \\
& \text{iff [induction]} \\
& \quad w \models_{\text{psl}}^c \mathfrak{M}(R_1) \text{ and } w \models_{\text{psl}}^c \mathfrak{M}(R_2) \\
& \text{iff } w \models_{\text{psl}}^c \{\mathfrak{M}(R_1)\} \ \&\& \ \{\mathfrak{M}(R_2)\} \\
& \text{iff } w \models_{\text{psl}}^c \{\{\mathfrak{M}(R_1)\} \ \&\& \ \{\mathfrak{M}(R_2)\}\} \\
& \text{iff } w \models_{\text{psl}}^c \mathfrak{M}((R_1 \text{ intersect } R_2))
\end{aligned}$$

- $R = R_1 [*0]$.

$$\begin{aligned}
& w \models_{\text{sva}} \langle \mathcal{Q}(c) R_1 [*0] \rangle \\
& \text{iff } w \models_{\text{sva}} (\langle \mathcal{Q}(c) R_1 \rangle) [*0] \\
& \text{iff } |w| = 0 \\
& \text{iff } w \models_{\text{psl}}^c \mathfrak{M}(R_1) [*0] \\
& \text{iff } w \models_{\text{psl}}^c \mathfrak{M}(R_1 [*0])
\end{aligned}$$

- $R = R_1 [*1:\$]$.

$$\begin{aligned}
& w \models_{\text{sva}} \langle \mathcal{Q}(c) R_1 [*1:\$] \rangle \\
& \text{iff } w \models_{\text{sva}} (\langle \mathcal{Q}(c) R \rangle) [*1:\$] \\
& \text{iff there exist } w_1, \dots, w_j, j \geq 1, \text{ such that } w = w_1 \cdots w_j \text{ and for all } i \text{ such that} \\
& \quad 1 \leq i \leq j, w_i \models_{\text{sva}} \langle \mathcal{Q}(c) R \rangle \\
& \text{iff [induction]} \\
& \quad \text{there exist } w_1, \dots, w_j, j \geq 1, \text{ such that } w = w_1 \cdots w_j \text{ and for all } i \text{ such that} \\
& \quad 1 \leq i \leq j, w_i \models_{\text{psl}}^c \mathfrak{M}(R) \\
& \text{iff [Lemma 0.2]} \\
& \quad w \models_{\text{psl}}^c \mathfrak{M}(R) [+] \\
& \text{iff } w \models_{\text{psl}}^c \mathfrak{M}(R_1 [*1:\$])
\end{aligned}$$

□

Proposition 2.2: Let R be an unlocked SVA sequence and let w be a finite word over Σ . Then the following are equivalent:

1. $w \models_{\text{sva}} \langle \textcircled{c} R \rangle$.
2. $w \models_{\text{psl}}^c \mathfrak{M}(R)$.
3. $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{M}(R)\textcircled{c}$.

Proof: 1 and 2 are equivalent by Proposition 2.1. 2 and 3 are equivalent by definition. □

Definition 2: Let b be a boolean expression, let R be an unlocked SVA sequence, and let S_1, S_2 be clocked SVA sequences.

- $\mathfrak{M}(\textcircled{c}(b) R) = \{\mathfrak{M}(R)\}\textcircled{c}b$
- $\mathfrak{M}((S_1 \## S_2)) = \{\mathfrak{M}(S_1) ; \mathfrak{M}(S_2)\}$

□

Proposition 2.3: Let S be a clocked SVA sequence and let w be a finite word over Σ . Then $w \models_{\text{sva}} \langle S \rangle$ iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{M}(S)$.

Proof: By induction over the structure of S .

- $S = \textcircled{c}(c) R$. The result follows from Proposition 2.2.
- $S = (S_1 \## S_2)$.

$$\begin{aligned}
& w \models_{\text{sva}} \langle (S_1 \## S_2) \rangle \\
& \text{iff } w \models_{\text{sva}} \langle \langle S_1 \rangle \## \langle S_2 \rangle \rangle \\
& \text{iff there exist } x, y \text{ such that } w = xy \text{ and } x \models_{\text{sva}} \langle S_1 \rangle \text{ and } y \models_{\text{sva}} \langle S_2 \rangle \\
& \text{iff [induction]} \\
& \quad \text{there exist } x, y \text{ such that } w = xy \text{ and } x \models_{\text{psl}}^{\text{TRUE}} \mathfrak{M}(S_1) \text{ and } y \models_{\text{psl}}^{\text{TRUE}} \mathfrak{M}(S_2) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(S_1) ; \mathfrak{M}(S_2)\} \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{M}((S_1 \## S_2))
\end{aligned}$$

□

3. Mapping unlocked SVA properties to unlocked PSL formulas

Since sequences can be properties, the letter “ \mathfrak{T} ” will be used instead of “ \mathfrak{M} ” to denote the mapping at the level of properties and assertions.

If φ is an unlocked SVA property and if “`disable iff (b) φ` ” is also an unlocked SVA property, then φ will be called an *unlocked SVA property fragment*.

Definition 3: Let b be a boolean expression, let R, R_1, R_2 be unlocked SVA sequences, and let φ be an unlocked SVA property fragment.

- $\mathfrak{I}(R) = \{\mathfrak{M}(R)\}!$
- $\mathfrak{I}(\text{not } R) = !\mathfrak{I}(R)$
- $\mathfrak{I}((R_1 \mid\text{-}\> R_2)) = \{\mathfrak{M}(R_1)\} \mid\text{-}\> \mathfrak{I}(R_2)$
- $\mathfrak{I}(\text{not}(R_1 \mid\text{-}\> R_2)) = !\mathfrak{I}((R_1 \mid\text{-}\> R_2))$
- $\mathfrak{I}((R_1 \mid\text{-}\> \text{not } R_2)) = \{\mathfrak{M}(R_1)\} \mid\text{-}\> \mathfrak{I}(\text{not } R_2)$
- $\mathfrak{I}(\text{not}(R_1 \mid\text{-}\> \text{not } R_2)) = !\mathfrak{I}((R_1 \mid\text{-}\> \text{not } R_2))$
- $\mathfrak{I}(\text{disable iff } (b) \varphi) = \mathfrak{I}(\varphi) \text{ abort } b$

□

Proposition 3.1: *Let φ be an unclocked SVA property fragment, and let w be a word over Σ . Then $w \models_{\text{sva}} \varphi$ iff $w \models_{\text{psl}} \mathfrak{I}(\varphi)$.*

Proof:

- $\varphi = R$.

$w \models_{\text{sva}} R$
 iff there exists $0 \leq j < |w|$ such that $w^{0..j} \models_{\text{sva}} R$
 iff [Proposition 1.1]
 there exists $0 \leq j < |w|$ such that $w^{0..j} \models_{\text{psl}} \mathfrak{M}(R)$
 iff $w \models_{\text{psl}} \{\mathfrak{M}(R)\}!$
 iff $w \models_{\text{psl}} \mathfrak{I}(R)$

- $\varphi = \text{not } R$.

$w \models_{\text{sva}} \text{not } R$
 iff $\bar{w} \not\models_{\text{sva}} R$
 iff [proof for $\varphi = R$]
 $\bar{w} \not\models_{\text{psl}} \mathfrak{I}(R)$
 iff $w \models_{\text{psl}} !\mathfrak{I}(R)$
 iff $w \models_{\text{psl}} \mathfrak{I}(\text{not } R)$

- $\varphi = (R_1 \mid\text{-}\> R_2)$.

$w \models_{\text{sva}} (R_1 \mid\text{-}\> R_2)$
 iff for every $0 \leq j < |w|$ such that $\bar{w}^{0..j} \models_{\text{sva}} R_1, w^{j..} \models_{\text{sva}} R_2$
 iff [Proposition 1.1, proof for $\varphi = R$]
 for every $0 \leq j < |w|$ such that $\bar{w}^{0..j} \models_{\text{psl}} \mathfrak{M}(R_1), w^{j..} \models_{\text{psl}} \mathfrak{I}(R_2)$
 iff $w \models_{\text{psl}} \{\mathfrak{M}(R_1)\} \mid\text{-}\> \mathfrak{I}(R_2)$
 iff $w \models_{\text{psl}} \mathfrak{I}((R_1 \mid\text{-}\> R_2))$

- $\varphi = \text{not}(R_1 \mid\text{-}\> R_2)$.

$w \models_{\text{sva}} \text{not}(R_1 \mid\text{-}\rightarrow R_2)$
iff $\bar{w} \not\models_{\text{sva}} (R_1 \mid\text{-}\rightarrow R_2)$
iff [proof for $\varphi = (R_1 \mid\text{-}\rightarrow R_2)$]
 $\bar{w} \not\models_{\text{psl}} \mathfrak{I}((R_1 \mid\text{-}\rightarrow R_2))$
iff $w \models_{\text{psl}} !\mathfrak{I}((R_1 \mid\text{-}\rightarrow R_2))$
iff $w \models_{\text{psl}} \mathfrak{I}(\text{not}(R_1 \mid\text{-}\rightarrow R_2))$

- $\varphi = (R_1 \mid\text{-}\rightarrow \text{not } R_2)$.

$w \models_{\text{sva}} (R_1 \mid\text{-}\rightarrow \text{not } R_2)$
iff for every $0 \leq j < |w|$ such that $\bar{w}^{0..j} \models_{\text{sva}} R_1, w^{j..} \models_{\text{sva}} \text{not } R_2$
iff [Proposition 1.1, proof for $\varphi = \text{not } R_1$]
for every $0 \leq j < |w|$ such that $\bar{w}^{0..j} \models_{\text{psl}} \mathfrak{M}(R_1), w^{j..} \models_{\text{psl}} \mathfrak{I}(\text{not } R_2)$
iff $w \models_{\text{psl}} \{\mathfrak{M}(R_1)\} \mid\text{-}\rightarrow \mathfrak{I}(\text{not } R_2)$
iff $w \models_{\text{psl}} \mathfrak{I}((R_1 \mid\text{-}\rightarrow \text{not } R_2))$

- $\varphi = \text{not}(R_1 \mid\text{-}\rightarrow \text{not } R_2)$.

$w \models_{\text{sva}} \text{not}(R_1 \mid\text{-}\rightarrow \text{not } R_2)$
iff $\bar{w} \not\models_{\text{sva}} (R_1 \mid\text{-}\rightarrow \text{not } R_2)$
iff [proof for $\varphi = (R_1 \mid\text{-}\rightarrow \text{not } R_2)$]
 $\bar{w} \not\models_{\text{psl}} \mathfrak{I}((R_1 \mid\text{-}\rightarrow \text{not } R_2))$
iff $w \models_{\text{psl}} !\mathfrak{I}((R_1 \mid\text{-}\rightarrow \text{not } R_2))$
iff $w \models_{\text{psl}} \mathfrak{I}(\text{not}(R_1 \mid\text{-}\rightarrow \text{not } R_2))$

□

Proposition 3.2: *Let φ be an unclocked SVA property fragment, let b be a boolean expression, and let w be a word over Σ . Then the following are equivalent:*

1. $w \models_{\text{sva}} \text{disable iff } (b) \varphi$.
2. $w \models_{\text{psl}} \mathfrak{I}(\text{disable iff } (b) \varphi)$.

Proof:

$w \models_{\text{sva}} \text{disable iff } (b) \varphi$
iff $w \models_{\text{sva}} \varphi$ or there exists $0 \leq k < |w|$ such that $w^k \models b$ and
 $w^{0..k-1} \top \models_{\text{sva}} \varphi$
iff [Proposition 3.1]
 $w \models_{\text{psl}} \mathfrak{I}(\varphi)$ or there exists $0 \leq k < |w|$ such that $w^k \models b$ and
 $w^{0..k-1} \top \models_{\text{psl}} \mathfrak{I}(\varphi)$
iff $w \models_{\text{psl}} \mathfrak{I}(\varphi) \text{ abort } b$
iff $w \models_{\text{psl}} \mathfrak{I}(\text{disable iff } (b) \varphi)$

□

Corollary 3.3: *Let P be an unlocked SVA property, and let w be a word over Σ . Then $w \models_{\text{sva}} P$ iff $w \models_{\text{psl}} \mathfrak{I}(P)$.*

Proof: If P is an unlocked SVA property fragment, then the result follows from Proposition 3.1. Otherwise, P has the form “**disable iff** (b) φ ”, where φ is an unlocked SVA property fragment, and the result follows from Proposition 3.2. □

4. Mapping clocked SVA properties to PSL formulas

Since sequences can be properties, the letter “ \mathfrak{I} ” will be used instead of “ \mathfrak{M} ” to denote the mapping at the level of properties and assertions.

If ψ is a clocked SVA property and if “**disable iff** (b) ψ ” is also a clocked SVA property, then ψ will be called a *clocked SVA property fragment*.

Definition 4: Let b, c be boolean expressions, let R, R_1, R_2 be unlocked SVA sequences, let φ be an unlocked SVA property fragment, let S, S_1, S_2 be clocked SVA sequences, and let ψ be a clocked SVA property fragment.

- $\mathfrak{I}(S) = \{\mathfrak{M}(S)\}!$
- $\mathfrak{I}(\text{not } S) = !\mathfrak{I}(S)$
- $\mathfrak{I}((S_1 \mid\rightarrow S_2)) = \{\mathfrak{M}(S_1)\} \mid\rightarrow \mathfrak{I}(S_2)$
- $\mathfrak{I}(\text{not}(S_1 \mid\rightarrow S_2)) = !\mathfrak{I}((S_1 \mid\rightarrow S_2))$
- $\mathfrak{I}((S_1 \mid\rightarrow \text{not } S_2)) = \{\mathfrak{M}(S_1)\} \mid\rightarrow \mathfrak{I}(\text{not } S_2)$
- $\mathfrak{I}(\text{not}(S_1 \mid\rightarrow \text{not } S_2)) = !\mathfrak{I}((S_1 \mid\rightarrow \text{not } S_2))$
- $\mathfrak{I}(\text{disable iff } (b) \psi) = \mathfrak{I}(\psi) \text{ abort } b$
- $\mathfrak{I}(@ (c) \text{ not } b) = \mathfrak{I}(@ (c) !b)$
- $\mathfrak{I}(@ (c) \text{ not } R) = !\mathfrak{I}(@ (c) R)$, provided R is not a boolean expression.
- $\mathfrak{I}(@ (c) (R_1 \mid\rightarrow R_2)) = \mathfrak{I}(@ (c) R_1 \mid\rightarrow @ (c) R_2)$
- $\mathfrak{I}(@ (c) \text{ not}(R_1 \mid\rightarrow R_2)) = !\mathfrak{I}(@ (c) (R_1 \mid\rightarrow R_2))$
- $\mathfrak{I}(@ (c) (R_1 \mid\rightarrow \text{not } b)) = \mathfrak{I}(@ (c) R_1 \mid\rightarrow @ (c) !b)$
- $\mathfrak{I}(@ (c) (R_1 \mid\rightarrow \text{not } R_2)) = \mathfrak{I}(@ (c) R_1 \mid\rightarrow \text{not } @ (c) R_2)$, provided R_2 is not a boolean expression.
- $\mathfrak{I}(@ (c) \text{ not}(R_1 \mid\rightarrow \text{not } R_2)) = !\mathfrak{I}(@ (c) (R_1 \mid\rightarrow \text{not } R_2))$
- $\mathfrak{I}(@ (c) \text{ disable iff } (b) \varphi) = \mathfrak{I}(@ (c) \varphi) \text{ abort } b$

□

Proposition 4.1: *Let ψ be a clocked SVA property fragment and let w be a word over Σ . Then $w \models_{\text{sva}} \psi$ iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(\psi)$.*

Proof:

- $\psi = S$.

$$\begin{aligned}
& w \models_{\text{sva}} S \\
& \text{iff } w \models_{\text{sva}} \langle S \rangle \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{sva}} \langle S \rangle \\
& \text{iff [Proposition 2.3]} \\
& \quad \text{there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{M}(S) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(S)\}! \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(S)
\end{aligned}$$

- $\psi = \text{not } S$.

$$\begin{aligned}
& w \models_{\text{sva}} \text{not } S \\
& \text{iff } w \models_{\text{sva}} \text{not } \langle S \rangle \\
& \text{iff } \bar{w} \not\models_{\text{sva}} \langle S \rangle \\
& \text{iff [proof for } \psi = S] \\
& \quad \bar{w} \not\models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(S) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} !\mathfrak{T}(S) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(\text{not } S)
\end{aligned}$$

- $\psi = (S_1 \mid\rightarrow S_2)$.

$$\begin{aligned}
& w \models_{\text{sva}} (S_1 \mid\rightarrow S_2) \\
& \text{iff } w \models_{\text{sva}} (\langle S_1 \rangle \mid\rightarrow \langle S_2 \rangle) \\
& \text{iff for every } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \models_{\text{sva}} \langle S_1 \rangle, w^{j..} \models_{\text{sva}} \langle S_2 \rangle \\
& \text{iff [Proposition 2.3, proof for } \psi = S] \\
& \quad \text{for every } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{M}(S_1), w^{j..} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(S_2) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(S_1)\} \mid\rightarrow \mathfrak{T}(S_2) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(\langle S_1 \mid\rightarrow S_2 \rangle)
\end{aligned}$$

- $\psi = \text{not}(S_1 \mid\rightarrow S_2)$.

$$\begin{aligned}
& w \models_{\text{sva}} \text{not}(S_1 \mid\rightarrow S_2) \\
& \text{iff } w \models_{\text{sva}} \text{not}(\langle S_1 \rangle \mid\rightarrow \langle S_2 \rangle) \\
& \text{iff } \bar{w} \not\models_{\text{sva}} (\langle S_1 \rangle \mid\rightarrow \langle S_2 \rangle) \\
& \text{iff [proof for } \psi = (S_1 \mid\rightarrow S_2)] \\
& \quad \bar{w} \not\models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(\langle S_1 \mid\rightarrow S_2 \rangle) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} !\mathfrak{T}(\langle S_1 \mid\rightarrow S_2 \rangle) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(\text{not}(S_1 \mid\rightarrow S_2))
\end{aligned}$$

- $\psi = (S_1 \mid\rightarrow \text{not } S_2)$.

$$\begin{aligned}
& w \models_{\text{sva}} (S_1 \mid\rightarrow \text{not } S_2) \\
& \text{iff } w \models_{\text{sva}} (\langle S_1 \rangle \mid\rightarrow \text{not } \langle S_2 \rangle) \\
& \text{iff for every } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \models_{\text{sva}} \langle S_1 \rangle, w^{j..} \models_{\text{sva}} \text{not } \langle S_2 \rangle \\
& \text{iff [Proposition 2.3, proof for } \psi = \text{not } S] \\
& \quad \text{for every } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{M}(S_1), w^{j..} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{not } S_2) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(S_1)\} \mid\rightarrow \mathfrak{I}(\text{not } S_2) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}((S_1 \mid\rightarrow \text{not } S_2))
\end{aligned}$$

- $\psi = \text{not}(S_1 \mid\rightarrow \text{not } S_2)$.

$$\begin{aligned}
& w \models_{\text{sva}} \text{not}(S_1 \mid\rightarrow \text{not } S_2) \\
& \text{iff } w \models_{\text{sva}} \text{not}(\langle S_1 \rangle \mid\rightarrow \text{not } \langle S_2 \rangle) \\
& \text{iff } \bar{w} \not\models_{\text{sva}} (\langle S_1 \rangle \mid\rightarrow \text{not } \langle S_2 \rangle) \\
& \text{iff [proof for } \psi = (S_1 \mid\rightarrow \text{not } S_2)] \\
& \quad \bar{w} \not\models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}((S_1 \mid\rightarrow \text{not } S_2)) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} !(\mathfrak{I}((S_1 \mid\rightarrow \text{not } S_2))) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{not}(S_1 \mid\rightarrow \text{not } S_2))
\end{aligned}$$

- $\psi = @(\bar{c}) \text{ not } b$.

$$\begin{aligned}
& w \models_{\text{sva}} @(\bar{c}) \text{ not } b \\
& \text{iff } w \models_{\text{sva}} \langle @(\bar{c}) \text{ not } b \rangle \\
& \text{iff } w \models_{\text{sva}} \langle @(\bar{c}) !b \rangle \\
& \text{iff [proof for } \psi = S] \\
& \quad w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@(\bar{c}) !b) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@(\bar{c}) \text{ not } b)
\end{aligned}$$

- $\psi = @(\bar{c}) \text{ not } R$, R not a boolean expression.

$$\begin{aligned}
& w \models_{\text{sva}} @(\bar{c}) \text{ not } R \\
& \text{iff } w \models_{\text{sva}} \langle @(\bar{c}) \text{ not } R \rangle \\
& \text{iff } w \models_{\text{sva}} \text{not } \langle @(\bar{c}) R \rangle \\
& \text{iff } \bar{w} \not\models_{\text{sva}} \langle @(\bar{c}) R \rangle \\
& \text{iff [proof for } \psi = S] \\
& \quad \bar{w} \not\models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@(\bar{c}) R) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} !\mathfrak{I}(@(\bar{c}) R) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@(\bar{c}) \text{ not } R)
\end{aligned}$$

- $\psi = @(\bar{c}) (R_1 \mid\rightarrow R_2)$.

$$\begin{aligned}
& w \models_{\text{sva}} @(\bar{c}) (R_1 \mid\rightarrow R_2) \\
& \text{iff } w \models_{\text{sva}} \langle @(\bar{c}) (R_1 \mid\rightarrow R_2) \rangle
\end{aligned}$$

iff $w \models_{\text{sva}} \langle \langle \mathbb{Q}(c) R_1 \rangle \mid \rightarrow \langle \mathbb{Q}(c) R_2 \rangle \rangle$
 iff [proof for $\psi = (S_1 \mid \rightarrow S_2)$]
 $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(\langle \mathbb{Q}(c) R_1 \mid \rightarrow \mathbb{Q}(c) R_2 \rangle)$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(\mathbb{Q}(c) (R_1 \mid \rightarrow R_2))$

- $\psi = \mathbb{Q}(c) \text{ not}(R_1 \mid \rightarrow R_2)$.

$w \models_{\text{sva}} \mathbb{Q}(c) \text{ not}(R_1 \mid \rightarrow R_2)$
 iff $w \models_{\text{sva}} \langle \mathbb{Q}(c) \text{ not}(R_1 \mid \rightarrow R_2) \rangle$
 iff $w \models_{\text{sva}} \text{not}(\langle \mathbb{Q}(c) R_1 \mid \rightarrow \langle \mathbb{Q}(c) R_2 \rangle \rangle)$
 iff [proof for $\psi = \text{not}(S_1 \mid \rightarrow S_2)$]
 $w \models_{\text{psl}}^{\text{TRUE}} !\mathfrak{T}(\langle \mathbb{Q}(c) R_1 \mid \rightarrow \mathbb{Q}(c) R_2 \rangle)$
 iff $w \models_{\text{psl}}^{\text{TRUE}} !\mathfrak{T}(\mathbb{Q}(c) (R_1 \mid \rightarrow R_2))$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(\mathbb{Q}(c) \text{ not}(R_1 \mid \rightarrow R_2))$

- $\psi = \mathbb{Q}(c) (R_1 \mid \rightarrow \text{not } b)$.

$w \models_{\text{sva}} \mathbb{Q}(c) (R_1 \mid \rightarrow \text{not } b)$
 iff $w \models_{\text{sva}} \langle \mathbb{Q}(c) (R_1 \mid \rightarrow \text{not } b) \rangle$
 iff $w \models_{\text{sva}} \langle \langle \mathbb{Q}(c) R_1 \rangle \mid \rightarrow \langle \mathbb{Q}(c) !b \rangle \rangle$
 iff [proof for $\psi = (S_1 \mid \rightarrow S_2)$]
 $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(\langle \mathbb{Q}(c) R_1 \mid \rightarrow \mathbb{Q}(c) !b \rangle)$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(\mathbb{Q}(c) (R_1 \mid \rightarrow \text{not } b))$

- $\psi = \mathbb{Q}(c) (R_1 \mid \rightarrow \text{not } R_2)$, R_2 not a boolean expression.

$w \models_{\text{sva}} \mathbb{Q}(c) (R_1 \mid \rightarrow \text{not } R_2)$
 iff $w \models_{\text{sva}} \langle \mathbb{Q}(c) (R_1 \mid \rightarrow \text{not } R_2) \rangle$
 iff $w \models_{\text{sva}} \langle \langle \mathbb{Q}(c) R_1 \rangle \mid \rightarrow \text{not } \langle \mathbb{Q}(c) R_2 \rangle \rangle$
 iff [proof for $\psi = (S_1 \mid \rightarrow \text{not } S_2)$]
 $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(\langle \mathbb{Q}(c) R_1 \mid \rightarrow \text{not } \mathbb{Q}(c) R_2 \rangle)$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(\mathbb{Q}(c) (R_1 \mid \rightarrow \text{not } R_2))$

- $\psi = \mathbb{Q}(c) \text{ not}(R_1 \mid \rightarrow \text{not } R_2)$.

$w \models_{\text{sva}} \mathbb{Q}(c) \text{ not}(R_1 \mid \rightarrow \text{not } R_2)$
 iff $w \models_{\text{sva}} \langle \mathbb{Q}(c) \text{ not}(R_1 \mid \rightarrow \text{not } R_2) \rangle$
 iff $w \models_{\text{sva}} \text{not}(\langle \mathbb{Q}(c) (R_1 \mid \rightarrow \text{not } R_2) \rangle)$
 iff $\bar{w} \not\models_{\text{sva}} \langle \mathbb{Q}(c) (R_1 \mid \rightarrow \text{not } R_2) \rangle$
 iff [proofs for $\psi = \mathbb{Q}(c) (R_1 \mid \rightarrow \text{not } R_2)$, R_2 boolean and not]
 $\bar{w} \not\models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(\mathbb{Q}(c) (R_1 \mid \rightarrow \text{not } R_2))$
 iff $w \models_{\text{psl}}^{\text{TRUE}} !\mathfrak{T}(\mathbb{Q}(c) (R_1 \mid \rightarrow \text{not } R_2))$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{T}(\mathbb{Q}(c) \text{ not}(R_1 \mid \rightarrow \text{not } R_2))$

□

Proposition 4.2: *Let ψ be a clocked SVA property fragment, let b be a boolean expression, and let w be a word over Σ . Then the following are equivalent:*

1. $w \models_{\text{sva}} \text{disable iff } (b) \psi$.
2. $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{disable iff } (b) \psi)$.

Proof:

$$\begin{aligned}
& w \models_{\text{sva}} \text{disable iff } (b) \psi \\
& \text{iff } w \models_{\text{sva}} \psi \text{ or there exists } 0 \leq k < |w| \text{ such that } w^k \models b \text{ and} \\
& \quad w^{0..k-1} \top \omega \models_{\text{sva}} \psi \\
& \text{iff [Proposition 4.1]} \\
& \quad w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\psi) \text{ or there exists } 0 \leq k < |w| \text{ such that } w^k \models b \text{ and} \\
& \quad w^{0..k-1} \top \omega \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\psi) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\psi) \text{ abort } b \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{disable iff } (b) \psi)
\end{aligned}$$

□

Corollary 4.3: *Let Q be a clocked SVA property and let w be a word over Σ . Then $w \models_{\text{sva}} Q$ iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(Q)$.*

Proof:

- $Q = @ (c) P$, where P is an unlocked SVA property. If P is an unlocked property fragment, then Q is a clocked SVA property fragment and the result follows from Proposition 4.1. Otherwise, P has the form “disable iff $(b) \varphi$ ”, where φ is an unlocked property fragment. In this case,

$$\begin{aligned}
& w \models_{\text{sva}} @ (c) \text{disable iff } (b) \varphi \\
& \text{iff } w \models_{\text{sva}} \text{disable iff } (b) @ (c) \varphi \\
& \text{iff [Proposition 4.2]} \\
& \quad w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{disable iff } (b) @ (c) \varphi) \\
& \text{iff } [\mathfrak{I}(\text{disable iff } (b) \psi) = \mathfrak{I}(\psi) \text{ abort } b] \\
& \quad w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@ (c) \varphi) \text{ abort } b \\
& \text{iff } [\mathfrak{I}(@ (c) \text{disable iff } (b) \varphi) = \mathfrak{I}(@ (c) \varphi) \text{ abort } b] \\
& \quad w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@ (c) \text{disable iff } (b) \varphi)
\end{aligned}$$

- $Q = \text{disable iff } (b) \psi$, where ψ is a clocked SVA property fragment. In this case, the result follows from Proposition 4.2.

□

5. Mapping SVA assertions to PSL formulas

The SVA assertion semantics is defined with respect to a boolean enabling condition. Therefore, the mapping must account for this enabling condition. “ \mathfrak{I}^b ” denotes the mapping when the SVA enabling condition is b .

Definition 5:

- $\mathfrak{I}^b(\text{always assert property } Q) = \text{always } (b \rightarrow \mathfrak{I}(Q))$
- $\mathfrak{I}^b(\text{always } @c \text{ assert property } P) = (\text{always } (b \rightarrow \mathfrak{I}(P))) @c$
- $\mathfrak{I}^b(\text{initial assert property } Q) = b! \rightarrow \mathfrak{I}(Q)$
- $\mathfrak{I}^b(\text{initial } @c \text{ assert property } P) = (\{b\} \mid \rightarrow \mathfrak{I}(P)) @c$

□

Lemma 5.1: *Let f be a PSL formula, let c be a boolean expression, and let w be a proper word over Σ . Then the following are equivalent:*

1. $w \models_{\text{psl}}^{\text{TRUE}} (\text{always } f) @c$
2. for all $0 \leq i < |w|$ such that $\bar{w}^i \models c$, $w^{i..} \models_{\text{psl}}^c f$

Proof:

$$\begin{aligned}
& w \models_{\text{psl}}^{\text{TRUE}} (\text{always } f) @c \\
& \text{iff } w \models_{\text{psl}}^c \text{always } f \\
& \text{iff } w \models_{\text{psl}}^c ![\text{TRUE U } !f] \\
& \text{iff } \bar{w} \not\models_{\text{psl}}^c [\text{TRUE U } !f] \\
& \text{iff } \neg(\text{there exists } 0 \leq k < |w| \text{ such that } \bar{w}^k \models c \text{ and } \bar{w}^{k..} \models_{\text{psl}}^c !f \text{ and for all } \\
& \quad 0 \leq j < k \text{ such that } w^j \models c, \bar{w}^{j..} \models_{\text{psl}}^c \text{TRUE}) \\
& \text{iff for all } 0 \leq k < |w| \text{ such that } \bar{w}^k \models c, \text{ either } \bar{w}^{k..} \not\models_{\text{psl}}^c !f \text{ or } \neg(\text{for all } \\
& \quad 0 \leq j < k \text{ such that } w^j \models c, \bar{w}^{j..} \models_{\text{psl}}^c \text{TRUE}) \\
& \text{iff for all } 0 \leq k < |w| \text{ such that } \bar{w}^k \models c, \text{ either } w^{k..} \models_{\text{psl}}^c f \text{ or there exists } \\
& \quad 0 \leq j < k \text{ such that } w^j \models c \text{ and } \bar{w}^{j..} \not\models_{\text{psl}}^c \text{TRUE} \\
& \text{iff } [\text{if } w^j \models c, \text{ then either } w^j \in 2^{\mathbf{P}}, \text{ in which case } \bar{w}^{j..} \models_{\text{psl}}^c \text{TRUE by Lemma} \\
& \quad 0.16, \text{ or } w^j = \top, \text{ in which case } w^k = \top \text{ (because } w \text{ is proper) and so} \\
& \quad \bar{w}^k \not\models c] \\
& \quad \text{for all } 0 \leq k < |w| \text{ such that } \bar{w}^k \models c, w^{k..} \models_{\text{psl}}^c f
\end{aligned}$$

□

Lemma 5.2: *Let f be a PSL formula, let b and c be boolean expressions, and let w be a word over Σ . Then the following are equivalent:*

1. $w \models_{\text{psl}}^c (b! @\text{TRUE}) \rightarrow f$
2. if $|w| > 0$ and $\bar{w}^0 \models b$, then $w \models_{\text{psl}}^c f$

If $|w| > 0$ and $\bar{w}^0 \models c$, then 1 and 2 are equivalent to

$$3. w \models_{\text{psl}}^c b! \rightarrow f$$

$$4. w \models_{\text{psl}}^c b \rightarrow f$$

If f is non-degenerate and w is proper, then 1 and 2 are equivalent to

$$5. w \models_{\text{psl}}^c \{b \text{ @TRUE}\} \mid \rightarrow f$$

If f is non-degenerate, w is proper, $|w| > 0$, and $\bar{w}^0 \models c$, then 1-5 are equivalent to

$$6. w \models_{\text{psl}}^c \{b\} \mid \rightarrow f$$

Proof:

$$\begin{aligned} & w \models_{\text{psl}}^c (b! \text{ @TRUE}) \rightarrow f \\ \text{iff } & w \models_{\text{psl}}^c !((b! \text{ @TRUE}) \ \&\& \ !f) \\ \text{iff } & \bar{w} \not\models_{\text{psl}}^c (b! \text{ @TRUE}) \ \&\& \ !f \\ \text{iff } & \bar{w} \not\models_{\text{psl}}^c b! \text{ @TRUE or } \bar{w} \not\models_{\text{psl}}^c !f \\ \text{iff } & \bar{w} \not\models_{\text{psl}}^{\text{TRUE}} b! \text{ or } w \models_{\text{psl}}^c f \\ \text{iff } & \text{if } \bar{w} \models_{\text{psl}}^{\text{TRUE}} b!, \text{ then } w \models_{\text{psl}}^c f \\ \text{iff } & \end{aligned}$$

(A):

if there exists $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of TRUE and $\bar{w}^j \models b$, then $w \models_{\text{psl}}^c f$

[(A) implies 2]: Assume (A). Assume $|w| > 0$ and $\bar{w}^0 \models b$. Then $\bar{w}^{0..0}$ is a clock tick of TRUE, so the precondition of (A) is satisfied with $j = 0$. Therefore $w \models_{\text{psl}}^c f$.

[2 implies (A)]. Assume 2. Assume that there exists $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of TRUE and $\bar{w}^j \models b$. Then $|w| > 0$. If $j = 0$, then $\bar{w}^0 \models b$. If $j > 0$, then by Lemma 0.1, $\bar{w}^0 = \top$, hence $\bar{w}^0 \models b$. Therefore the precondition of 2 is satisfied, and so $w \models_{\text{psl}}^c f$.

This proves that 1 and 2 are equivalent. Suppose now that $|w| > 0$ and $\bar{w}^0 \models c$.

$$\begin{aligned} & w \models_{\text{psl}}^c b! \rightarrow f \\ \text{iff } & w \models_{\text{psl}}^c !((b!) \ \&\& \ !f) \\ \text{iff } & \bar{w} \not\models_{\text{psl}}^c (b!) \ \&\& \ !f \\ \text{iff } & \bar{w} \not\models_{\text{psl}}^c b! \text{ or } \bar{w} \not\models_{\text{psl}}^c !f \\ \text{iff } & \bar{w} \not\models_{\text{psl}}^c b! \text{ or } w \models_{\text{psl}}^c f \\ \text{iff } & \text{if } \bar{w} \models_{\text{psl}}^c b!, \text{ then } w \models_{\text{psl}}^c f \\ \text{iff } & \end{aligned}$$

(B):

if (there exists $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of c and $\bar{w}^j \models b$), then $w \models_{\text{psl}}^c f$

[(B) implies 2]: Assume (B). Assume $|w| > 0$ and $\bar{w}^0 \models b$. Since $\bar{w}^0 \models c$, $\bar{w}^{0..0}$ is a clock tick of c , so by (B), $w \models_{\text{psl}}^c f$.

[2 implies (B)]. Assume 2. Suppose that $0 \leq j < |w|$ is such that $\bar{w}^{0..j}$ is a clock tick of c and $\bar{w}^j \models b$. Then $|w| > 0$. If $j = 0$, then $\bar{w}^0 \models b$. If $j > 0$, then $\bar{w}^0 \models !c$. Since $\bar{w}^0 \models c$, $\bar{w}^0 = \top$, and so $\bar{w}^0 \models b$. Therefore the precondition of 2 is satisfied, and so $w \models_{\text{psl}}^c f$.

This proves that 2 and 3 are equivalent if $|w| > 0$ and $\bar{w}^0 \models c$.

$$\begin{aligned}
& w \models_{\text{psl}}^c b \rightarrow f \\
& \text{iff } w \models_{\text{psl}}^c !(b \ \&\& \ !f) \\
& \text{iff } \bar{w} \not\models_{\text{psl}}^c b \ \&\& \ !f \\
& \text{iff } \bar{w} \not\models_{\text{psl}}^c b \text{ or } \bar{w} \not\models_{\text{psl}}^c !f \\
& \text{iff } \bar{w} \not\models_{\text{psl}}^c b \text{ or } w \models_{\text{psl}}^c f \\
& \text{iff [Lemma 0.16, using } |w| > 0 \text{ and } \bar{w}^0 \models c] \\
& \quad \bar{w} \not\models_{\text{psl}}^c b! \text{ or } w \models_{\text{psl}}^c f \\
& \text{iff [proof of equivalence of 2 and 3]} \\
& \text{(B)}
\end{aligned}$$

Since (B) was shown equivalent to 2 when $|w| > 0$ and $\bar{w}^0 \models c$, this proves that 2 and 4 are equivalent when $|w| > 0$ and $\bar{w}^0 \models c$.

Suppose now that f is non-degenerate and w is proper.

$$\begin{aligned}
& w \models_{\text{psl}}^c \{b \ \text{@TRUE}\} \mid \rightarrow f \\
& \text{iff for all } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \models_{\text{psl}}^c b \ \text{@TRUE}, w^{j..} \models_{\text{psl}}^c f \\
& \text{iff for all } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \models_{\text{psl}}^{\text{TRUE}} b, w^{j..} \models_{\text{psl}}^c f \\
& \text{iff} \\
& \text{(C):} \\
& \text{for all } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \text{ is a clock tick of TRUE and } \bar{w}^j \models b, \\
& w^{j..} \models_{\text{psl}}^c f
\end{aligned}$$

[(C) implies 2]: Assume (C). Assume $|w| > 0$ and $\bar{w}^0 \models b$. Then $\bar{w}^{0..0}$ is a clock tick of TRUE, so by (C), $w = w^{0..} \models_{\text{psl}}^c f$.

[2 implies (C)]. Assume 2. Suppose that $0 \leq j < |w|$ is such that $\bar{w}^{0..j}$ is a clock tick of TRUE and $\bar{w}^j \models b$. If $j > 0$, then $\bar{w}^0 \models \text{FALSE}$, hence $\bar{w}^0 = \top$. Therefore, $\bar{w}^0 \models b$, and so by 2, $w \models_{\text{psl}}^c f$. On the other hand, since w is proper and $w^0 = \perp, w = \perp^\omega$, and since f is non-degenerate, $w \not\models_{\text{psl}}^c f$, a contradiction. Therefore, $j = 0$ and $\bar{w}^0 \models b$, and so by 2, $w^{j..} = w \models_{\text{psl}}^c f$.

This proves that 2 and 5 are equivalent when f is non-degenerate and w is proper.

Suppose now that f is non-degenerate, w is proper, $|w| > 0$, and $\bar{w}^0 \models c$.

$$\begin{aligned}
& w \models_{\text{psl}}^c \{b\} \mid \rightarrow f \\
& \text{iff for all } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \models_{\text{psl}}^c b, w^{j..} \models_{\text{psl}}^c f \\
& \text{iff} \\
& \text{(D):} \\
& \text{for all } 0 \leq j < |w| \text{ such that } \bar{w}^{0..j} \text{ is a clock tick of } c \text{ and } \bar{w}^j \models b, \\
& w^{j..} \models_{\text{psl}}^c f
\end{aligned}$$

[(D) implies 2]: Assume (D). Assume $|w| > 0$ and $\bar{w}^0 \models b$. Since $\bar{w}^0 \models c$, $\bar{w}^{0..0}$ is a clock tick of c , so by (D), $w \models_{\text{psl}}^c f$.

[2 implies (D)]. Assume 2. Suppose that $0 \leq j < |w|$ is such that $\bar{w}^{0..j}$ is a clock tick of c and $\bar{w}^j \models b$. If $j > 0$, then $\bar{w}^0 \models !c$. Since $\bar{w}^0 \models c$, we must have $\bar{w}^0 = \top$. Therefore, $\bar{w}^0 \models b$, and so by 2, $w \models_{\text{psl}}^c f$. On the other hand, since w is proper and $w^0 = \perp$, $w = \perp^\omega$, and since f is non-degenerate, $w \not\models_{\text{psl}}^c f$, a contradiction. Therefore, $j = 0$ and $\bar{w}^0 \models b$, and so by 2, $w^{j..} = w \models_{\text{psl}}^c f$.

This proves that 2 and 6 are equivalent when f is non-degenerate, w is proper, $|w| > 0$, and $\bar{w}^0 \models c$. □

Lemma 5.3: *Let f be a PSL formula, let b and c be boolean expressions, and let w be a proper word over Σ . Then the following are equivalent:*

1. for all $0 \leq j < |w|$ such that $\bar{w}^j \models c$ and $\bar{w}^j \models b$, $w^{j..} \models_{\text{psl}}^c f$
2. $w \models_{\text{psl}}^{\text{TRUE}} (\text{always}(b! \rightarrow f)) @c$
3. $w \models_{\text{psl}}^{\text{TRUE}} (\text{always}(b \rightarrow f)) @c$

If f is non-degenerate, then 1-3 are equivalent to

4. $w \models_{\text{psl}}^{\text{TRUE}} (\text{always}(\{b @\text{TRUE}\} \rightarrow f)) @c$
5. $w \models_{\text{psl}}^{\text{TRUE}} (\text{always}(\{b\} \rightarrow f)) @c$

Proof:

$$\begin{aligned}
& w \models_{\text{psl}}^{\text{TRUE}} (\text{always}(b! \rightarrow f)) @c \\
& \text{iff [Lemma 5.1]} \\
& \quad \text{for all } 0 \leq j < |w| \text{ such that } \bar{w}^j \models c, w^{j..} \models_{\text{psl}}^c b! \rightarrow f \\
& \text{iff [Lemma 5.2]} \\
& \quad \text{for all } 0 \leq j < |w| \text{ such that } \bar{w}^j \models c, \text{ if } \bar{w}^j \models b, \text{ then } w^{j..} \models_{\text{psl}}^c f \\
& \text{iff for all } 0 \leq j < |w| \text{ such that } \bar{w}^j \models c \text{ and } \bar{w}^j \models b, w^{j..} \models_{\text{psl}}^c f
\end{aligned}$$

This proves the equivalence of 1 and 2. A similar argument proves the equivalence of 1 and 3.

$$\begin{aligned}
& w \models_{\text{psl}}^{\text{TRUE}} \text{always}(\{b @\text{TRUE}\} \rightarrow f) @c \\
& \text{iff [Lemma 5.1]} \\
& \quad \text{for all } 0 \leq j < |w| \text{ such that } \bar{w}^j \models c, w^{j..} \models_{\text{psl}}^c \{b @\text{TRUE}\} \rightarrow f \\
& \text{iff [Lemma 5.2]} \\
& \quad \text{for all } 0 \leq j < |w| \text{ such that } \bar{w}^j \models c, \text{ if } \bar{w}^j \models b, \text{ then } w^{j..} \models_{\text{psl}}^c f \\
& \text{iff for all } 0 \leq j < |w|, \text{ if } \bar{w}^j \models c \text{ and } \bar{w}^j \models b \text{ then } w^{j..} \models_{\text{psl}}^c f
\end{aligned}$$

This proves the equivalence of 1 and 4 when f is non-degenerate. A similar argument proves the equivalence of 1 and 5 when f is non-degenerate. □

Lemma 5.4: *Let c be a boolean expression, let P be an unclocked SVA property, and let w be a non-empty word over Σ such that $\bar{w}^0 \models c$. Then $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@c) P$ iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(P) @c$.*

Proof:

- $P = R$.

$$\begin{aligned}
& w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@c) R \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(@c) R\}! \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{M}(@c) R \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(R)\} @c \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^c \mathfrak{M}(R) \\
& \text{iff } w \models_{\text{psl}}^c \{\mathfrak{M}(R)\}! \\
& \text{iff } w \models_{\text{psl}}^c \mathfrak{I}(R) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(R) @c
\end{aligned}$$

- $P = \text{not } b$.

$$\begin{aligned}
& w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@c) \text{not } b \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@c) !b \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(@c) !b\}! \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{M}(@c) !b \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(!b)\} @c \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^c \mathfrak{M}(!b) \\
& \text{iff there exists } 0 \leq j < |w| \text{ such that } w^{0..j} \models_{\text{psl}}^c !b \\
& \text{iff [using the notation from Lemma 0.13]} \\
& \quad w \models_{\text{psl}}^c [!b]! \\
& \text{iff [Lemma 0.15, using } |w| > 0 \text{ and } \bar{w}^0 \models c] \\
& \quad w \models_{\text{psl}}^c [!b] \\
& \text{iff [Lemma 0.13]} \\
& \quad w \models_{\text{psl}}^c !(b!) \\
& \text{iff [Lemma 0.14]} \\
& \quad w \models_{\text{psl}}^c !(\{b\}!) \\
& \text{iff } w \models_{\text{psl}}^c !\mathfrak{I}(b) \\
& \text{iff } w \models_{\text{psl}}^c \mathfrak{I}(\text{not } b) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{not } b) @c
\end{aligned}$$

- $P = \text{not } R$, R not a boolean expression.

$$\begin{aligned}
& w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@c) \text{not } R \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} !\mathfrak{I}(@c) R \\
& \text{iff } \bar{w} \not\models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@c) R \\
& \text{iff [proof for } P = R] \\
& \quad \bar{w} \not\models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(R) @c \\
& \text{iff } \bar{w} \not\models_{\text{psl}}^c \mathfrak{I}(R)
\end{aligned}$$

iff $w \models_{\text{psl}}^c \text{!}\mathfrak{I}(R)$
 iff $w \models_{\text{psl}}^c \mathfrak{I}(\text{not } R)$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{not } R) \textcircled{c}$

- $P = (R_1 \mid\text{-}\> R_2)$.

$w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\textcircled{c} (R_1 \mid\text{-}\> R_2))$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\textcircled{c} R_1 \mid\text{-}\> \textcircled{c} R_2)$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(\textcircled{c} R_1)\} \mid\text{-}\> \mathfrak{I}(\textcircled{c} R_2)$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{M}(\textcircled{c} R_1)$, $w^{i..} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\textcircled{c} R_2)$
 iff [proof for $P = R$]
 for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{M}(\textcircled{c} R_1)$, $w^{i..} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(R_2) \textcircled{c}$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(R_1)\} \textcircled{c}$, $w^{i..} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(R_2) \textcircled{c}$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \{\mathfrak{M}(R_1)\}$, $w^{i..} \models_{\text{psl}}^c \mathfrak{I}(R_2)$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \mathfrak{M}(R_1)$, $w^{i..} \models_{\text{psl}}^c \mathfrak{I}(R_2)$
 iff $w \models_{\text{psl}}^c \{\mathfrak{M}(R_1)\} \mid\text{-}\> \mathfrak{I}(R_2)$
 iff $w \models_{\text{psl}}^c \mathfrak{I}(R_1 \mid\text{-}\> R_2)$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}((R_1 \mid\text{-}\> R_2)) \textcircled{c}$

- $P = \text{not}(R_1 \mid\text{-}\> R_2)$.

$w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\textcircled{c} \text{not}(R_1 \mid\text{-}\> R_2))$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \text{!}\mathfrak{I}(\textcircled{c} (R_1 \mid\text{-}\> R_2))$
 iff $\bar{w} \not\models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\textcircled{c} (R_1 \mid\text{-}\> R_2))$
 iff [proof for $P = (R_1 \mid\text{-}\> R_2)$]
 $\bar{w} \not\models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}((R_1 \mid\text{-}\> R_2)) \textcircled{c}$
 iff $\bar{w} \not\models_{\text{psl}}^c \mathfrak{I}((R_1 \mid\text{-}\> R_2))$
 iff $w \models_{\text{psl}}^c \text{!}\mathfrak{I}((R_1 \mid\text{-}\> R_2))$
 iff $w \models_{\text{psl}}^c \mathfrak{I}(\text{not}(R_1 \mid\text{-}\> R_2))$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{not}(R_1 \mid\text{-}\> R_2)) \textcircled{c}$

- $P = (R_1 \mid\text{-}\> \text{not } b)$.

$w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\textcircled{c} (R_1 \mid\text{-}\> \text{not } b))$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\textcircled{c} R_1 \mid\text{-}\> \textcircled{c} \text{!}b)$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{M}(\textcircled{c} R_1)$, $w^{i..} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\textcircled{c} \text{!}b)$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(R_1)\} \textcircled{c}$,
 $w^{i..} \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(\textcircled{c} \text{!}b)\} \textcircled{c}$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \{\mathfrak{M}(R_1)\}$, $w^{i..} \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(\text{!}b) \textcircled{c}\} \textcircled{c}$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \mathfrak{M}(R_1)$, $w^{i..} \models_{\text{psl}}^{\text{TRUE}} \{\text{!}b \textcircled{c}\} \textcircled{c}$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \mathfrak{M}(R_1)$, there exists $i \leq j < |w|$ such
 that $w^{i..j} \models_{\text{psl}}^{\text{TRUE}} \text{!}b \textcircled{c}$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \mathfrak{M}(R_1)$, there exists $i \leq j < |w|$ such
 that $w^{i..j} \models_{\text{psl}}^c \text{!}b$

iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \mathfrak{M}(R_1)$, $w^{i..} \models_{\text{psl}}^c \{!b\}!$
 iff [Lemma 0.14, using the notation of Lemma 0.13]
 for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \mathfrak{M}(R_1)$, $w^{i..} \models_{\text{psl}}^c [!b]!$
 iff [by Lemma 0.11, if $\bar{w}^{0..i} \models_{\text{psl}}^c \mathfrak{M}(R_1)$, then $\bar{w}^i \models c$, hence by Lemma 0.15,
 $w^{i..} \models_{\text{psl}}^c [!b]!$ iff $w^{i..} \models_{\text{psl}}^c [!b]$]
 for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \mathfrak{M}(R_1)$, $w^{i..} \models_{\text{psl}}^c [!b]$
 iff [Lemma 0.13]
 for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \mathfrak{M}(R_1)$, $w^{i..} \models_{\text{psl}}^c !(b!)$
 iff [Lemma 0.14]
 for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \mathfrak{M}(R_1)$, $w^{i..} \models_{\text{psl}}^c !(\{b\}!)$
 iff $w \models_{\text{psl}}^c \{\mathfrak{M}(R_1)\} \mid \rightarrow !(\{b\}!)$
 iff $w \models_{\text{psl}}^c \{\mathfrak{M}(R_1)\} \mid \rightarrow !(\{\mathfrak{M}(b)\}!)$
 iff $w \models_{\text{psl}}^c \{\mathfrak{M}(R_1)\} \mid \rightarrow !\mathfrak{I}(b)$
 iff $w \models_{\text{psl}}^c \{\mathfrak{M}(R_1)\} \mid \rightarrow \mathfrak{I}(\text{not } b)$
 iff $w \models_{\text{psl}}^c \mathfrak{I}((R_1 \mid \rightarrow \text{not } b))$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}((R_1 \mid \rightarrow \text{not } b)) @c$

- $P = (R_1 \mid \rightarrow \text{not } R_2)$, R_2 not a boolean expression.

$w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@c) (R_1 \mid \rightarrow \text{not } R_2)$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@c) (R_1 \mid \rightarrow \text{not } @c) (R_2)$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(@c) R_1\} \mid \rightarrow \mathfrak{I}(\text{not } @c) (R_2)$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \{\{\mathfrak{M}(R_1)\} @c\} \mid \rightarrow !\mathfrak{I}(@c) (R_2)$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^{\text{TRUE}} \{\mathfrak{M}(R_1)\} @c$,
 $w^{i..} \models_{\text{psl}}^{\text{TRUE}} !\mathfrak{I}(@c) (R_2)$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \{\mathfrak{M}(R_1)\}$, $w^{i..} \models_{\text{psl}}^{\text{TRUE}} !\mathfrak{I}(@c) (R_2)$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \mathfrak{M}(R_1)$, $\bar{w}^{i..} \not\models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@c) (R_2)$
 iff [proof for $P = R$]
 for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \mathfrak{M}(R_1)$, $\bar{w}^{i..} \not\models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(R_2) @c$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \mathfrak{M}(R_1)$, $\bar{w}^{i..} \not\models_{\text{psl}}^c \mathfrak{I}(R_2)$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c \mathfrak{M}(R_1)$, $w^{i..} \models_{\text{psl}}^c !\mathfrak{I}(R_2)$
 iff $w \models_{\text{psl}}^c \{\mathfrak{M}(R_1)\} \mid \rightarrow !\mathfrak{I}(R_2)$
 iff $w \models_{\text{psl}}^c \{\mathfrak{M}(R_1)\} \mid \rightarrow \mathfrak{I}(\text{not } R_2)$
 iff $w \models_{\text{psl}}^c \mathfrak{I}((R_1 \mid \rightarrow \text{not } R_2))$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}((R_1 \mid \rightarrow \text{not } R_2)) @c$

- $P = \text{not}(R_1 \mid \rightarrow \text{not } R_2)$.

$w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@c) \text{not}(R_1 \mid \rightarrow \text{not } R_2)$
 iff $w \models_{\text{psl}}^{\text{TRUE}} !(\mathfrak{I}(@c) (R_1 \mid \rightarrow \text{not } R_2))$
 iff $\bar{w} \not\models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@c) (R_1 \mid \rightarrow \text{not } R_2)$
 iff [proofs for $P = (R_1 \mid \rightarrow \text{not } R_2)$, R_2 boolean and not]
 $\bar{w} \not\models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}((R_1 \mid \rightarrow \text{not } R_2)) @c$
 iff $\bar{w} \not\models_{\text{psl}}^c \mathfrak{I}((R_1 \mid \rightarrow \text{not } R_2))$
 iff $w \models_{\text{psl}}^c !\mathfrak{I}((R_1 \mid \rightarrow \text{not } R_2))$
 iff $w \models_{\text{psl}}^c \mathfrak{I}(\text{not}(R_1 \mid \rightarrow \text{not } R_2))$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{not}(R_1 \mid \rightarrow \text{not } R_2)) @c$

- $P = \text{disable}$ iff $(b) \varphi$, φ an SVA unlocked property fragment.

$$\begin{aligned}
& w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{@}(c) \text{ disable iff } (b) \varphi) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{@}(c) \varphi) \text{ abort } b \\
& \text{iff either } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{@}(c) \varphi) \text{ or there exists } 0 \leq i < |w| \text{ such that } w^i \models b \text{ and} \\
& \quad w^{0..i-1} \top^\omega \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{@}(c) \varphi) \\
& \text{iff [proofs for the various forms of } \varphi] \\
& \quad \text{either } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\varphi) \text{@}c \text{ or there exists } 0 \leq i < |w| \text{ such that } w^i \models b \text{ and} \\
& \quad w^{0..i-1} \top^\omega \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\varphi) \text{@}c \\
& \text{iff either } w \models_{\text{psl}}^c \mathfrak{I}(\varphi) \text{ or there exists } 0 \leq i < |w| \text{ such that } w^i \models b \text{ and} \\
& \quad w^{0..i-1} \top^\omega \models_{\text{psl}}^c \mathfrak{I}(\varphi) \\
& \text{iff } w \models_{\text{psl}}^c \mathfrak{I}(\varphi) \text{ abort } b \\
& \text{iff } w \models_{\text{psl}}^c \mathfrak{I}(\text{disable iff } (b) \varphi) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{disable iff } (b) \varphi) \text{@}c
\end{aligned}$$

□

Proposition 5.1: *Let A be an SVA assertion, let b be a boolean expression, and let w be a proper word over Σ . Then the following are equivalent:*

1. $w, b \models_{\text{sva}} A$.
2. $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}^b(A)$.

Proof: Q denotes a clocked SVA property, and P denotes an unlocked SVA property.

- $A = \text{always assert property } Q$.

$$\begin{aligned}
& w, b \models_{\text{sva}} \text{always assert property } Q \\
& \text{iff for all } 0 \leq i < |w| \text{ such that } \bar{w}^i \models b, w^{i..} \models_{\text{sva}} Q \\
& \text{iff [Corollary 4.3]} \\
& \quad \text{for all } 0 \leq i < |w| \text{ such that } \bar{w}^i \models b, w^{i..} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(Q) \\
& \text{iff [Lemma 5.3, with } c = \text{TRUE}] \\
& \quad w \models_{\text{psl}}^{\text{TRUE}} \text{always } (b \rightarrow \mathfrak{I}(Q)) \text{@TRUE} \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \text{always } (b \rightarrow \mathfrak{I}(Q)) \\
& \text{iff } w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}^b(\text{always assert property } Q)
\end{aligned}$$

- $A = \text{always @}(c) \text{ assert property } P$.

$$\begin{aligned}
& w, b \models_{\text{sva}} \text{always @}(c) \text{ assert property } P \\
& \text{iff for all } 0 \leq i < |w| \text{ such that } \bar{w}^i \models c \text{ and } \bar{w}^i \models b, w^{i..} \models_{\text{sva}} \text{@}(c) P \\
& \text{iff [Corollary 4.3, with } Q = \text{@}(c) P] \\
& \quad \text{for all } 0 \leq i < |w| \text{ such that } \bar{w}^i \models c \text{ and } \bar{w}^i \models b, w^{i..} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(\text{@}(c) P) \\
& \text{iff [Lemma 5.4]}
\end{aligned}$$

for all $0 \leq i < |w|$ such that $\bar{w}^i \models c$ and $\bar{w}^i \models b$, $w^{i..} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(P) @c$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^i \models c$ and $\bar{w}^i \models b$, $w^{i..} \models_{\text{psl}}^c \mathfrak{I}(P)$
 iff [Lemma 5.3]
 $w \models_{\text{psl}}^{\text{TRUE}} \text{always } (b \rightarrow \mathfrak{I}(P)) @c$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}^b(\text{always } @c) \text{ assert property } P$

- $A = \text{initial assert property } Q$. First note that

$w \models_{\text{psl}}^{\text{TRUE}} b! \rightarrow f$
 iff [proof of Lemma 5.2]
 if (there exists $0 \leq j < |w|$ such that $\bar{w}^{0..j}$ is a clock tick of TRUE and $\bar{w}^j \models b$), then $w \models_{\text{psl}}^{\text{TRUE}} f$
 iff [Lemma 0.1]
 if (there exists $0 \leq j < |w|$ such that $\bar{w}^j \models b$ and $\bar{w}^i = \top$ for all $0 \leq i < j$),
 then $w \models_{\text{psl}}^{\text{TRUE}} f$
 iff [if $j > 0$, then $\bar{w}^0 = \top \models b$]
 if ($|w| > 0$ and $\bar{w}^0 \models b$), then $w \models_{\text{psl}}^{\text{TRUE}} f$

Now

$w, b \models_{\text{sva}} \text{initial assert property } Q$
 iff if $|w| > 0$ and $\bar{w}^0 \models b$, then $w \models_{\text{sva}} Q$
 iff [Corollary 4.3]
 if $|w| > 0$ and $\bar{w}^0 \models b$, then $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(Q)$
 iff [argument above]
 $w \models_{\text{psl}}^{\text{TRUE}} b! \rightarrow \mathfrak{I}(Q)$
 iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}^b(\text{initial assert property } Q)$

- $A = \text{initial } @c) \text{ assert property } P$.

$w, b \models_{\text{sva}} \text{initial } @c) \text{ assert property } P$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{sva}} !c[*0:\$] \#\#1 c$ and $\bar{w}^i \models b$,
 $w^{i..} \models_{\text{sva}} @c) P$
 iff [the proof of Proposition 2.1, case $R = b$, shows that
 $\bar{w}^{0..i} \models_{\text{sva}} !c[*0:\$] \#\#1 c$ iff $\bar{w}^{0..i}$ is a clock tick of c]
 for all $0 \leq i < |w|$ such that $\bar{w}^{0..i}$ is a clock tick of c and $\bar{w}^i \models b$,
 $w^{i..} \models_{\text{sva}} @c) P$
 iff [Corollary 4.3, with $Q = @c) P$]
 for all $0 \leq i < |w|$ such that $\bar{w}^{0..i}$ is a clock tick of c and $\bar{w}^i \models b$,
 $w^{i..} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@c) P$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c b$, $w^{i..} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(@c) P$
 iff [Lemma 5.4]
 for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c b$, $w^{i..} \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}(P) @c$
 iff for all $0 \leq i < |w|$ such that $\bar{w}^{0..i} \models_{\text{psl}}^c b$, $w^{i..} \models_{\text{psl}}^c \mathfrak{I}(P)$
 iff $w \models_{\text{psl}}^c \{b\} \mapsto \mathfrak{I}(P)$

iff $w \models_{\text{psl}}^{\text{TRUE}} (\{b\} \mapsto \mathfrak{I}(P)) @c$
iff $w \models_{\text{psl}}^{\text{TRUE}} \mathfrak{I}^b(\text{initial } @c \text{ assert property } P)$

□